International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 6, Issue 2, March - April 2017 ISSN 2278-6856

Design Trends in Cyber Security with Combined Approach

[1]Sandeep Kulkarni, [2]Dr. K. P. Yadav

[1]R/S Himalayan University, Arunachal Pradesh

[2]IIMT College of Engineering, Greater Noida

Introduction

In a world driven more and more by big data, social networks, online transactions, information stored or managed via internet and automated processes performed through the use of IT systems, information security and data privacy are permanently facing risks. With the development of new tools and techniques, cyber-crime is consistently increasing in terms of number of attacks and level of damage caused to its victims. IT-security experts engage 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.Cybercrime issues are related with the problems like security of financial dealings, prohibiting maltreatment of credit card information, providing security for information during online transactions, preserving privacy and confidentiality of e-mails and the attack on privacy. This growth has attracted hundreds of online companies to conduct business in the Middle East and allowed many existing sectors, such as education, health, airline, and government, to move their operations online.

Keywords: Targeted Attacks, Steganography, Visual attacks, Structural attacks , Cyber Bullying Various types and reasons of cyber crimes .

Mobile: Mobile attack is eating the world and becoming the dominant channel for instant communication and the expressway for banking and commerce worldwide. The combination of biometric technology integrated with risk-based authentication services is enabling a new generation of authentication services to replace passwords and PINs while meeting the needs of end users to deliver security in a way that is simple and seamless. RSA anticipates a growth in deployment of risk-based authentication services coupled with biometrics in the next one to three years as organizations look to minimize fraud losses as they move more services to the mobile channel.

Ransom ware: The virtual equivalent of real world extortion is increasingly the subject of both media coverage and incidence with an average payment of $500 to the "ransomeers" to release your data. The reason ransomware has become so popular for attackers all converges around the same thing: it makes money easily, singularly, and in almost every case, payment is guaranteed as organizations and individuals respond to fear.

Card-Not-Present Fraud Will Spike: With EMV chip cards gradually replacing the magnetic stripe, cybercriminals are rushing to gain the most they can financially before the U.S. goes almost completely over to them. As a result, ATMs and other POS terminals across the country are under attack from so-called skimming devices. EMV technology is hardly new and has been widely used across Europe and Asia for the past decade. This has provided cybercriminals with a ten year head start in developing mechanisms to work around the chip.

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. 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.

Crimes based on Personal Issue: Sometimes reasons of cybercrime are unintentional and by mistake. People unknowingly just for fun may send an email or make unauthorized access to another user's space. A Person may Steal the identity of his higher authority and can steal the confidential data for black money. A psychologically sick person may disseminate malicious software or viruses to harm other people being sick from progress of his/her colleagues. Social media Chat rooms may be another common place of cyber crime where children are mostly found soliciting and Abused . The FBI keep watching frequently the Chat rooms to stop this.

Man in the middle attack: It occurs when the attacker interferes between the two communication ends, thus every message sent from source A to source B reaches the attacker before reaching its destination. The risks further posed by this type of attack comprise of unauthorised access to sensitive information or possibilities to alter the information/message that reaches the destination by the attacker.

Targeted Attacks: Targeted attacks are the attacks that exploit some kind of vulnerabilities in popular software for compromising specific target systems & are becoming increasingly common. Such attacks are neither automated nor are they conducted by amateurs. These types of attacks may be well coordinated and include a series of failed and success compromises or a broader campaign, with the prime aim of obtaining sensitive data. The network was named GhostNet as the attackers used a Remote Access Trojan called ghostRAT.

Steganography: There exists a large number of image steganography techniques which are accompanied by various attacks on the steganography systems.
Visual attacks: All well-known techniques do not create any visible mark on the stego image. However, when the LSB plane is filtered to remove the significant part of the cover image, the difference becomes obvious. The technique like LSBM embeds data, irrespective to the nature and structure of image damaged texture in the LSB plane. One of the reasons to use edge-based steganography is to preserve the texture in the LSB plane.
Structural attacks : Embedding data in an image leads to statistical modification in the structure of cover image. Any such modification in a cover image can be observed by first- and second-order statistics. SP analysis and WS are two popular structural attacks. Both SP and WS estimate the length of the embedded message by giving the percentage of pixels which may hold data.

Types of Cyber-Crime That Are Committed Against Women: It involves invading the privacy by following a person's movements across the Internet by posting messages on the bulletin boards, entering the chat-rooms frequented by the victim, constantly bombarding the victim with messages and emails with obscene language.

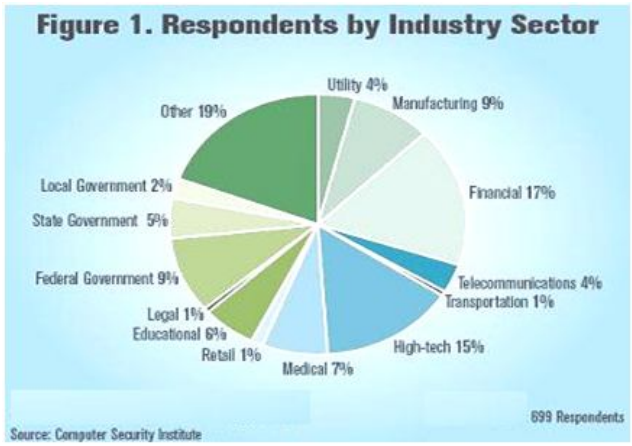
a) In Cyber Stalking, stalker access the victim's personal information like name, family background, telephone numbers and daily routine of the victim and post them on the websites related to dating services with the name of victim.
b) Harassment Via Email : One form may include Harassment through e-mails includes blackmailing, threatening, bullying, constant sending of love letters in anonymous names or regular sending of embarrassing mails to one's mail box.
c) Cyber Bullying: Cyber bullying is "willful and repeated harm inflicted through the use of computers, cell phones or other electronic devices, by sending messages of an intimidating or threatening nature.

d) Morphing: Morphing is editing the original picture by an unauthorized user. When unauthorized user with fake identity downloads victim's pictures and then uploads or reloads them after editing is known as morphing.

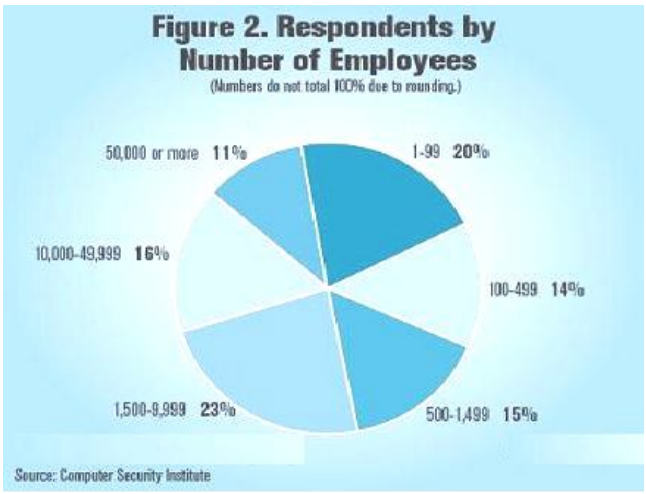
e) Cyber Defamation :The term defamation is used to define the injury that is caused to the reputation of a person in the eyes of a third person Cyber defamation is publishing of defamatory material against another person with the help of computers or internet.

Survey Results:

As figure shows malware effected organizations covered by the survey include many areas from both the private and public sectors.



The size of the malware affected organizations, as measured by number of employees that are represented in the survey can be seen in figure



Prevention from Attacks and Detecting Attacks:
Some security threats handled by CERT-IN are: Website Intrusion and Malware Propagations
Trojan Cryptolocker
Zero Access Botnet

Tracking of Open Proxy Servers : CERT-In has tracked more than 2000 open proxy servers existing in India and alerted concerned system administrators to properly configure them so as to

reduce spamming and other related malicious activities originating from India.

Botnet Tracking and Mitigation: Bots and Botnets involving Indian systems by CERTIn.

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.

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. As Middle East organizations expand their use of advanced security technology and use the latest hardware and software, it is becoming more difficult to conduct technical attacks. Similarly, the organizations are developing well-written complete security policies and hiring IT security experts that are also helping in reducing the number of possible attacks. Unfortunately, little is used to secure the weakest link, i.e. the users. This is pushing attackers to gain unauthorized access to information by exploiting user's trust and tendency to help. The paper discussed the security awareness among users in the Middle East and reported the findings of several IT security awareness studies conducted among students and professionals in UAE. It discussed the importance of assessing the security awareness by running controlled audits. 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. 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] Aparna Viswanathan Cyber Law
[2] An Introduction to Cyber Crime and Cyber Law.Author(s) : Dr R K Chaubey
[3] Cyber Crime Criminal Threats From Cyberspace.Author(s) : Susan W Brenner
[4] Cyber Crime and Corporate Liability.Author(s) : Rohas Nagpal
[5] Software Vulnerabilities, Banking Threats, Botnets and Malware Self-Protection Technologies by Wajeb Gharibi1, Abdulrahman Mirza ,2011
[6] McAfee Labs, 2012. Threats Predictions 2013, description available at: http://mcaffee.com
[7] Indian Express (2012) "Cyber bullying new-age threat" Indian Express.
[8] Cyber Crime and Cyber Security: A White Paper for Franchisors, Licensors, and Others by Bruce S. Schaeffer, Henfree Chan,Henry Chan and Susan Ogulnick
[9] MIT Geospatial Data Centre, 2013. Cyber security and human psychology.
[10] McAfee Labs, 2013. Threats Predictions 2014, description available at: http://mcaffee.com
[11] Didwania, P (2013) "India: Cyber Defamation In Corporate World" available on http:/ / www. mondaq.com/india/x/218890/Social+Media/Cyber+Defamation+In+Corporate+Word
[12] Cyber Crime 2015 https://www.emc.com/collateral/white-paper/rsa-white-paper-cybercrime-trends-2015.pdf
[13] Research on Improved ECC Algorithm in Network and Information Security.
[14] An Improved Weighted Clustering for Ad-hoc Network Security New by Basant Kumar Verma and Binod Kumar ,2015
[15] Network Security with Cryptography by Prof. Mukund R. Joshi, Renuka Avinash Karkade , 2015
[16] Network Security: Hybrid IDPS by Youssef Senhaji and Hicham Medromi , 2015
[17] Research on Computer Network Virus Defense Technology in Cloud Technology E18] Computer Network Security and Attacks on Wireless Sensor Network,Hacking issues by Sonal R.Jathe ,Dipti S. Charjan,Pallavi A.Patil,2016