Mehran University Research Journal of Engineering & Technology
Vol. 37, No. 2, 359-366, April 2018
p-ISSN: 0254-7821, e-ISSN: 2413-7219
DOI: 10.22581/muet1982.1802.12

Cyber Threats/Attacks and a Defensive Model to Mitigate Cyber Activities

JAWAD HUSSAIN AWAN*†, SHAHZAD MEMON*, SHEERAZ MEMON**,KAMRAN TAJ PATHAN* AND NIAZ HUSSAIN ARIJO*

RECEIVED ON 20.02.2017 ACCEPTED ON 21.08.2017

ABSTRACT

Nowadays, every internet user is part of cyber world. In this way, millions of users, knowledge seekers, and service provider organizations are connected to each other, a vast number of common people shifted their everyday activities to cyber world as they can save their time, traffic problem and gets effective and costless services by using various services such as, online banking, social networking sites, government services and cloud services. The use of Cyber services, eBusiness, eCommerce and eGovernance increases the usage of online/cyber services also increased the issue of cyber security. Recently, various cases have been reported in the literature and media about the cyber-attacks and crimes which seriously disrupted governments, businesses and personal lives. From the literature. It is noticed that every cyber user is unaware about privacy and security practices and measures. Therefore, cyber user has provided knowledge and fully aware them from the online services and also about cyber privacy and security. This paper presents a review on the recent cybercrimes, threats and attacks reported in the literature and media. In addition, the impact of these cyber breaches and cyber law to deal with cyber security has been discussed. At last, a defensive model is also proposed to mitigate cyber-criminal activities.

Key Words: Cyber Security, Cyber Crime, Internet, Threats.

1. INTRODUCTION

In this information age, the internet is an integrated part of our daily life. It is an online source, which provides speedy communication to the whole world, organizations and people are connected through various cyber services such as eBanking, eGovernment services, social media, edutainment and cloud services [1]. These services are available without time and location barriers so the dependence on these services in last few years [2]. However, with many benefits, the cyber security is an emerging challenge to all these online/cyber services.

Consequently, cyber criminals are making target to most usable and accessible cyber services. In this manner, online fraud, child pornography, hacking, violations of IPR (Intellectual Property Rights) are major cyber-attacks, which are increasing day by day. Furthermore, it is also

†Corresponding Author (E-Mail: jawad.awan@scholars.usindh.edu.pk)
* Institute of Information & Communication Technology, University of Sindh, Jamshoro
** Department of Computer Systems Engineering, Mehran University of Engineering & Technology, Jamshoro

reported in [3] that the confidential information of south Korean employee have been theft and approximately 80 million credit cards were stolen, these credit cards includes income utilization reports and card numbers. In addition, researchers have dedicated to address the cyber security issues, challenges and providing suggested or recommended solutions for these domains to make them more secure for users, employers, customers, organization and governments.

This paper contributes a review of current cybercrimes and threats which can seriously affect the modern world's essential, interactive and user-friendly cyber services. In addition, it concludes with some recommended suggestions which are suggested by cyber policy maker and emerging technology designing organizations (such as: Microsoft) which can be adopted to minimize the cyber-attacks and also increase the awareness among cyber users of this emerging world. Further, this paper is divided into eight sections. Section I discusses about the Introduction, Literature review is discussed in section 2, categories of cyber criminals are illustrated in section 3, cybercrimes, threats and attacks are discussed in section 4, a novel model is proposed in Section 5, cyber protection laws and strategies are discussed in section 6 and conclusion is discussed in section 7.

2. LITERATURE REVIEW

In cyber era, increasing number of emerging technologies increases the issues concerned with the privacy and security of their offered services [4-5]. Furthermore, it is reported and noticed that US is one of those countries where credit card fraud became daily issue and now reached at 47% of the whole world [6]. These frauds show the failure of government policies because the citizens of US rely on older, malfunctioning technology and the remaining countries have upgraded their technology [4]. These credit cards comprise of magnetic stripes where person's financial and confidential information is programmed [5]. This magnetic stripe is simple to replicate and cyber criminals do that after stealing. While other countries embedded small chips into credit cards (Such as EMV (Euro pay Master Card and Visa). Those are more secure because each transaction is assigned a random number that changes simultaneously when customers use their credit card. So, skilled hackers are installing malicious programs remotely onto departing terminals of retail stores where credit card numbers are being captured to breech the security of these credit cards. In this way, cyber criminals get user's financial and confidential information and sell that information to the highest bidder for their financial interest. Drive-by exploits [7] are also the most spreading malicious form of online threats, which happen when a malware is downloaded onto an internet user's computer while visiting infected websites as well as drive-by exploit targets a victim's computer for their interest without the his/her authorization. Nowadays, drive-by exploits is used as cybercrime tool by cyber criminals and malware actors. F-Secure, Symantec and Kaspersky designed EPP (Endpoint Protection) products which offer robust defenses against drive-by exploit. It is also examined that these products block these types of attacks (Approximately 100%). EPP products play an important role to block the infected websites while a user visits the infected websites as well as blacklist those infected websites to avoid visiting again. Latest EPP products have some features of real-time, look-ups, cloud-security which are aggressive and making quick decisions when an infected website is loaded. In addition, Zombie malware [8-9] is also used for attacks. This Zombie creates a background running program without any awareness of user that the cyber attacker is going to tap his/her computing device to spread attacks in the form of spam, viruses and spyware across this cyber world. Gradually, number of Zombie malware is increasing. It is happening because of malicious email attachments or some activities

downloaded by drive-by which creates an action and Trojan virus is installed in user's computer.

3. CATEGORIES OF CYBER CRIMINALS

In this section, some of the Cyber-criminals have been categorized as below and shown in Fig. 1 [10-11]:

Hacker: Hacker is a special computer operator, who seeks and exploits weaknesses in a computer system or computer network. These individuals explore others' computer systems for education, eCommerce, or information system.

Crackers: Cracker is a computer literate person, who has broad computer knowledge and aims to breach internet security and get access to information system without paying any cost.

Cyber Terrorists: Cyber terrorist is also a programmer, who breaches computer system security to steal or destroy cyber user information for cyber-terrorism purpose. Smart hacker hacks government websites which is also a form of cyber terrorism.

Salami Attackers: These attackers use an online database to grab the customer's confidential information such as bank and credit card details and targeting them for financial crimes. For example: a new custom designed program is inserted by bank employee into bank's servers, which deducts a small amount from customer's account.

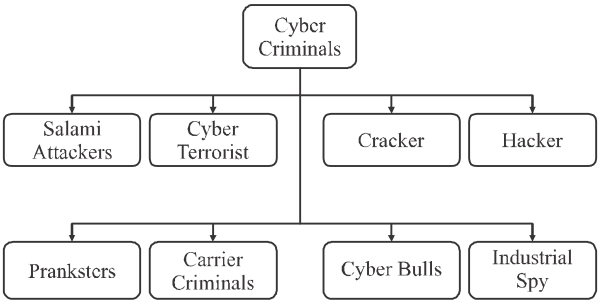

FIG. 1. CATEGORIES OF CYBER ATTACKERS IN 2014

Pranksters: Pranksters are least malicious computer criminals who aim to harm computer system and financial data lost to individual or a group or an organization.

Career Criminals: Career criminals earn their income from criminal activities, while they are dissatisfied, devotees and useless people. They work within skilful groups such as the APT17. Most of career criminals are found in Russia, Italy, and Asia.

Cyber Bulls: Cyber bulls harass cyber users via the Internet. He/she uploads fake posts on forums, posting fake profiles on social sites (Such as Face book, WhatsApp), sending malicious email messages.

Industrial Spy: Industrial spy is the person who attempts to access information about future plans of company or secrets of trade.

4. CYBER THREATS, ATTACKSAND CRIMES

In this section, current cyber threats, attacks have been discussed as under in following sub-sections:

4.1 Cyber Threats and Attacks

According to TrapX Security, which is a deception-based cyber security defense company reported a hijacking technique named as "MEDJACK" by which medical devices are hijacked [12]. Before targeting to healthcare industry, attackers have to be attentive and informative about vulnerable entry point of medical devices. It is further reported by Ponemon Institute that $6 billion is the estimated amount which has been breached. Furthermore, it is acknowledged that PACS (Picture Archive and Communications Systems) were the targeted points from where attackers targeted attack. Because PACS provides images from multiple devices, such as CT (Computed Tomography), MRI (Magnetic

Resonance Imaging), X-Ray to hospitals radiology department and which are associated to the hospital's entire network [13]. Currently, malicious actors are focusing medical areas (such as medical industries, hospitals) because medical records are highly valuable on the black market and malicious actors have targeted the healthcare industry in 2014 [12]. In [14], CBC (Canadian Broadcasting Corporation) News and National Security Agency reported that Five Eyes (Such as: Spy Agencies) have been planned to hack and corrupt Google and Samsung's app stores. Thus, Google is securing its services by upgrading their security features. Besides, UC Browser is also globally usable mobile browser which is mostly used by operating systems such as Android, BlackBerry and Symbian and UC Browser became one of the world's primary intermediary mobile browser, which is risen up to 13% of the market need with 500 million users. Because of this, it is reported that it is under threat and may be future target of the cyber criminals. Thus, its security is also challenging for cyber users.

4.2 Cyber Attacks Reported

From the report [7], it is reported and illustrated in Fig. 2(a-b) that USA is the world most cyber-attack suffering country where 47.40% attacks have been taken place in the month of May 2015. Such as username and password hacking is on the top of list, DNS hijacking where bank's websites are directed to rogue websites, deface of Sherriff's department official website and leaked employee's records, law enforcement, sending of malwares in healthcare systems and more. UK is on 2nd rank where 7.90% cyber-attacks took place, jamming of the cars standing at car parking areas, DDoS (Distributed Denial of Service) attacks on education institutes (Such as University of London Computer Centre). Belgium and Thailand are on 3rd rank which reached at 5.30%. Belgium lost 87,000$ after attack of malware via email. In Thailand, leakage of government website login credentials happened. Some countries such as New Zealand, Saudi Arabia, India, Italy, Hong Kong, Japan, Nepal, Canada and other having 2.63% cyber-attack ratio in which some countries websites are hacked, stealing of government information and in most of countries confidential information of employees , staff and their customers have been stolen.

4.3 Crime Report 2016 and 2017

From the report [15], it has been noticed that the economic crime in 2016 varies and effects the economy of the country. More, the reported affected ratio of economy in % have been mentioned as under in **Table 1** as Africa 50% Western Europe 35% North America 41% Eastern Europe 39% Asia Pacific 32% Latin America 35% Middle East 21% Global 36%.

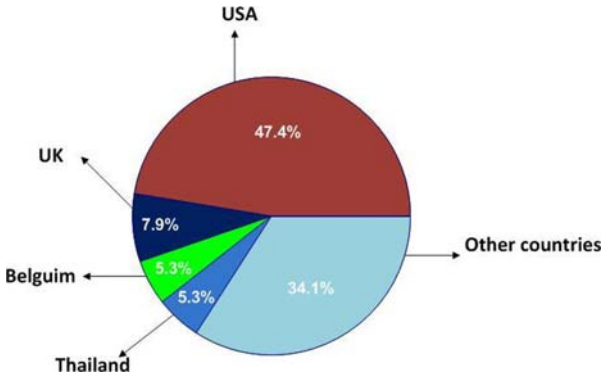

FIG. 2(a). CYBER ATTACKS IN 2015

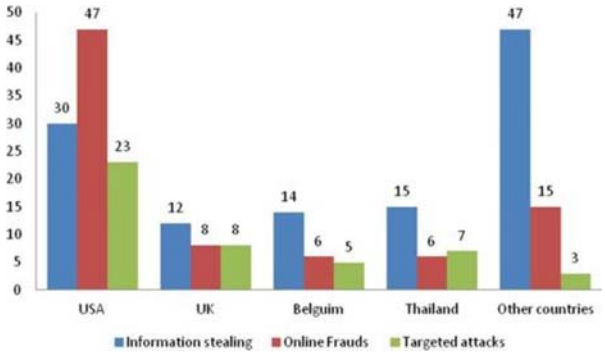

FIG. 2(b). COUNTRY WISE CYBER ATTACKS IN 2015

Furthermore, some economic crimes such as Asset misuse 64% Cyber-criminal activities 32% enticement dishonesty 24% Procurement fraud 23% Financial fraud 18% HR fraud 12% currency launder case 11% IP breach 7% Insider trade 7% Tax fraud 6% credit fraud 6% Competition/anti-trust rule breach 4% spying 2% and other activities 11% [15] have been illustrated in Fig. 3.

4.4 Types of Cyber Crimes

In this sub section, cybercrimes along with their objective and examples are discussed which are shown in Table 2.

5. PROPOSED MODEL

From the collected literature, surveys and research studies, it is noticed that the cyber era is facing the problem of the privacy and security of cyber services, networks and integrated technologies. To overcome or deal to this issue, a security model is proposed. This proposed model contains the merged features of Zed Attack proxy, W3af, web securify. The model has an internal working mechanism which may take four steps to process the requested task. In this mechanism, Step-1 loads system requested URL, after that goes for second step which scans URL and analyze the compatibility of applications. In step three and step four monitors the threats, attacks and vulnerabilities after that lists them along with applied actions shown in Fig. 4. This model also has a testing mechanism, which may comprise of four phases. First phase contains the information of server and client technologies, software and configuration practices. Phase two scan and results cyber threats, attacks and vulnerabilities by using brute force, fuzzing technique or manually. Phase three verifies that the target is vulnerable, measures attack effectiveness, ease of exploitability. Phase four assists in document findings, lists improvement and present examples.

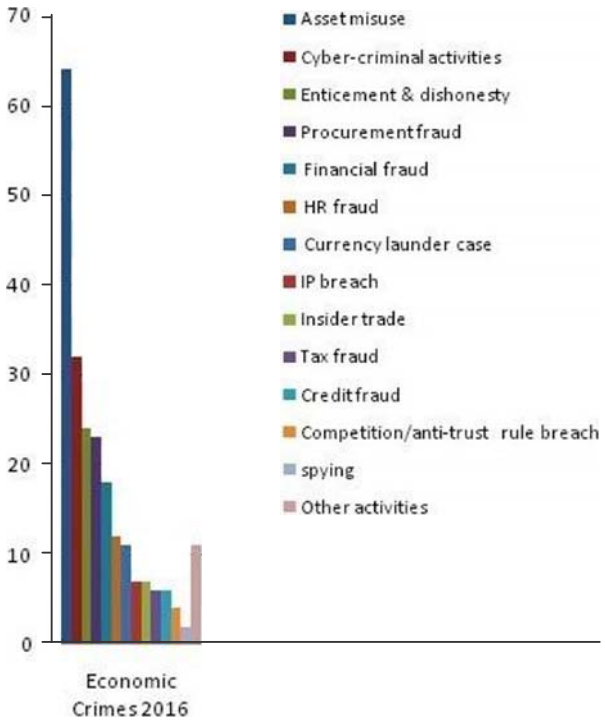

FIG. 3. ECONOMIC CRIMES 2016 AND 2017

TABLE 1. ECONOMIC CRIME REPORT 2016 & 2017

No.	Country	Economy Affected(%)
1.	Africa	50
2.	Western Europe	35
3.	North America	41
4.	Eastern Europe	39
5.	Asia Pacific	32
6.	Latin America	35
7.	Middle East	21
8.	Global	36

6. CYBER PROTECTION LAWS AND STRATEGIES

In 2015, lawmakers have reintroduced the "Aaron's Law" to decline the increasing number of cyber-attacks and threats [16]. Aaron's Law was first introduced and sent for acceptance in 2013, but failed to pass. The aim of lawmakers is limit the possibility of the existing anti-hacking act and control prosecutorial action for assured CFAA (Computer Fraud and Abuse Act) violations. Furthermore, it is stated that Aaron's Law is one-step forward into the 21st Century, which cannot fix all exploiting activities those done by cyber criminals, hackers and others. Fire Eye and Microsoft [17] have stopped a scheme, where malicious activities are hidden by IT pro forum of cybercriminal group known as APT17 in China. APT17 group infects machine with the help of Black Coffee malware. This malware uses IT forum pages and TechNet (Microsoft product) profiles. Command-and-control server performs malicious activities on an infected machine which are operated by online criminals. It is simple and easy to attack a computer or machine because of this number of groups grown to choose the legal purposes of famous websites in order to encode their command-and-control communications. From this report, it is noticed that APT17 used Google and Bing to conceal their activities and host locations in the past.

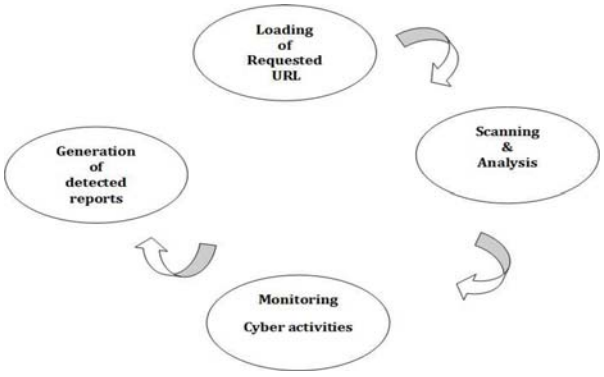

FIG. 4. WORKING MECHANISM OF PROPOSED MODEL

TABLE 2. TYPES OF CYBER CRIMES ALONG WITH THEIR OBJECTIVES

Type of Cyber Crime	Objective
Hacking	Hacking is an approach by which a computer system or computer network is exploited.
Cyber Stalking	It is a method of harassment by which an individual, a group, or an organization is harassed via internet.
Phishing	Phishing is an e-mail fraud trick which is used for the identity theft or information.
Email Spoofing	Email spoofing is an online activity which is helpful to createemail messages with a fake sender address.
Cyber Terrorism	Cyber terrorism is one of the current emerging issues where terrorist activities, Such as large-scale disruption of computer networks are carried out via internet.
Piracy	Piracy is an act of criminal violence which is linked with copyright violation.
Theft	Theft is intentional activity by which a person's property is taken or used without his/her consent to deny its legal proprietor.
Fraud	Fraud is a type of criminal activity or prejudicing someone's rights for personal gain.
Distributed Denial of Service	An Activity which hides available resources of a machine or network for its future users.
Harassment	Intended threatening behavior
Mail Bomb	Mail bomb is an internet activity by which a bunch of e-mail are sent to a specific user or system to hang the functioning of server.

7. CONCLUSION

In the age of digital cyber world, cyber and information security is an emerging field in these days where a large number of user's score increasing day by day where new and high equipped cyber technologies and their services are offered by different public and private organization which are being targeted by cyber criminals also. This paper illustrates and highlights latest cybercrimes, criminal activists, cyber threats and attacks along with a report for the awareness of cyber users, which may be helpful to mitigate cybercrimes, attacks/ threats. The users may be secured from them by using and applying proposed security model and also practices of security cyber laws and strategies. It is also noticed that appropriate education is essential for cyber users to decrease cybercrime activities regarding cybercrime and defensive measures. In this paper, cyber criminals have been categorized to make cyber user aware from their objectives as well as cyber protection laws and strategies are suggested to make cyber users secure. Moreover, research surveys using latest tools, trainings and other efficient mechanism should be adopted to extend awareness amongst the cyber service user and also train them about their privileges and responsibilities regarding the cyber services and information systems.

ACKNOWLEDGEMENT

Authors are thankful to the Director, Institute of Information & Communication Technology, University of Sindh, Jamshoro, Pakistan, for providing Information Technology Laboratory and Digital Library, access facility to accomplish this research.

REFERENCES

[1] Memon, S.A., and Awan, J.H., "Transformation Towards Cyber Democracy: A Study on Contemporary Policies, Practices and Adoption Challenges for Pakistan", Handbook of Cyber-Development, Cyber-Democracy and Cyber-Defense, pp. 50-51, Switzerland, 2017.

[2] Awan, J.H., Memon, S., Khan, R.A., Noonari, A.Q., Hussain, Z., and Usman, M., "Security Strategies to Overcome Cyber Measures, Factors and Barriers", Engineering Science Technology, International Research Journal, Volume 1, No. 1, pp. 51-58, Pakistan, 2017.

[3] "Massive Data Theft in South Korea Highlights Financial Cybersecurity Weakness [2014-01-20] Security Magazine", [Online]. Available: http://www.securitymagazine.com/articles/85139-massive-data-theft-in-south-korea-highlights-financial-cybersecurity-weakness. [Accessed: 9th June, 2015].

[4] Awan, J.H., Memon, S., Shah, M., and Awan, F.H., "eGovernment Services Security and Challenges in Pakistan", SAI Computing, pp. 1082-1085, UK, 2016.

[5] Awan, J.H., and Memon, S., "Threats of Cyber Security and Challenges for Pakistan", 11th International Conference on Cyber Warfare and Security, Boston, pp. 425, USA, 2016.

[6] "47% of the World's Credit Card Fraud Happens in the US [2015-06-01] Security Magazine", [Online]. Available: http://www.securitymagazine.com/articles/86413-of-the-worlds-credit-card-fraud-happens-in-the-us. [Accessed: 9th June, 2015].

[7] "Report: Top Endpoint Security Packages Perfectly Foil Drive-By Attacks." [Online]. Available: http://www.technewsworld.com/story/82009.html. [Accessed: 9th June, 2015].

[8] Dawson, M., Omar, M., and Abramson, J., "Understanding the Methods behind Cyber Terrorism", pp. 5270, USA, January, 2015.

[9] "Containing the Zombie Malware Outbreak." [Online]. Available: http://www.technewsworld.com/story/82090.html. [Accessed: 9th June, 2015].

[10] Broadhurst, R., Grabosky, P., Alazab, M., and Chon, S., "Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime", International Journal of Cyber Criminol, Volume 8, No. 1, pp. 1-20, Australia, 2014.

[11] Hemraj, S., Rao, Y.S., and Panda, T.C., "Cyber-Crimes and their Impacts: A Review", International Journal of Engineering Research and Applications, Volume 2, pp. 202-209, India, 2012.

[12] "Medical Devices Used as Pivot Point in Hospital Attacks: Report|SecurityWeek.Com." [Online]. Available: http://www.securityweek.com/medical-devices-used-pivot-point-hospital-attacks-report. [Accessed: 9th Jun, 2015].

[13] Awan, J.H., Memon, S.A., Memon, N.A., Shah, R., Bhutto, Z., and Khan, R.A., "Conceptual Model for WWBAN (Wearable Wireless Body Area Network)", International Journal of Advanced Computer Science Applied, Volume 8, No. 1, pp. 377-381, UK, 2017.

[14] "Spy Agencies Planned to Corrupt Google Play." [Online]. Available: http://www.technewsworld.com/story/82091.html. [Accessed: 9th June, 2015].

[15] Mcllheney, C., and McCotter, S., "Global Economic Crime Survey", UK , 2016.

[16] "Cyber Security Strategy: The Government of Japan", Japan, 2015.

[17] "FireEye, Microsoft Outsmart Clever Chinese Malware" [Online]. Available: http://www.technewsworld.com/story/82060.html. [Accessed: 9th June, 2015].