International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 78.96 | Impact Factor (2016): 6.391

Critical Infrastructure Protection of ICT in Muslim World

Sami Mohammed Abdulrahman Ali[1], Muhammad Abdu[2], Jamaludin Bin Ibrahim[3]

Department of Information System, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia

Abstract: ***This paper explain about many Muslim world get cyber cyberattack ,how vulnerable critical infrastructure protection especially in cyber in Muslim country such as Malaysia, Saudi Arabia, Turkey, and UAE compare to the west country , in this paper we know that most Muslim country are more vulnerable than west world because some reason. We recommend possible suggestions to reduce the effect of cyberattacks in Muslim countries.***

Keywords: Muslim Countries, critical, infrastructure, protection, cyber, crime

1. Introduction

In era technology internet most critical infrastructure using network to doing daily operation, it's so important protect this critical infrastructure. Critical infrastructure is assets that are vital for the functioning of an economy and society for country. Critical infrastructure have many different form like Wastewater Systems Sector, Transportation Systems, Materials, and Waste Sector, Information Technology Sector, Government Facilities Sector, Healthcare and Public Health Sector, Financial Services Sector, Food and Agriculture Sector Emergency Services Sector, Energy Sector, Dams Sector, Defense Industrial Base Sector, Communications Sector, Commercial Facilities Sector, Chemical Sector. All of this sector need to be protected. Disruptions of this sector could result in disastrous, loss of life, economic effects and significant harm to citizen.

Critical infrastructure is being attack every day and study about that already be conducted .this attack become increase day by day. Many reason behind this attack, it can be economy reason, sabotage, political reason, or only just test skill. Muslim country for example Malaysia is being attacked by some country mainly reason it's because economy reason. This hacker using network to disturb financial service sector in Malaysia. Most of them want to steal money from financial service sector. Another example is from Turkey most attack come from Europe because of political reason. This attacker try to hacking government website. Thus, from all those example we need to conduct recommendation system and policy to protect country from various attack. Commonly recognized cyber-aggressors include (Fischer, 2013):

- Cyber-terrorists: a radical people who engage in cyber-attacks as a form of warfare to cause extensive destruction.
- Cyber-spies: thieving specific information from government or private sectors to get competitive strategic or political advantage.
- Cyber-thieves: thieving specific information from governments or private for monetary gain.
- Cyber-warriors: representatives to who develop capabilities and undertake cyber-attacks in Achieve political objectives.
- Cyber-hacktivists who execute cyber-attacks for fun, or nonmonetary reasons.

2. Previous work

Many study was conducted before about importance of manage security in critical infrastructure sector .According to (watts, 2005) critical infrastructure systems central to the everyday operation of government, financial and well-being are already under attack, and trends show them these attacks will continue to increase in number in year. With era of Internet expands, this attack will become more increase. Even though this threat always increase every time government have seemed relative low to slow to respond (Ashraf, 2015).

As connectivity increases in the world protection from cyber-attack is extremely important. Protection cyber-attack is can be describe as a cybersecurity shield designed to offers secure intercommunication among the elements of a system, and to frustrate any attempt at disruption by any other countries, terrorist organizations, or hacker groups with hostile intentions. Because of the frequency of cyber-attacks on the country's critical infrastructure cybersecurity professionals have a greater role to in securing critical infrastructures (Shwani, 2014). (Xiaoxue Liu, Jiexin Zhang,Peidong Zhu, 2016) Study that not only critical infrastructure network (CIN) but also cyber physical security (CPS) are important to maintain good security in this area.

(Gouglidis, B. Green, J. Busby, M. Rouncefield, D. Hutchison and S. Schauer, 2016) Show that the protection of critical infrastructures is not a single problem but rather a multi-variable problem. From this point Gouglidis et al, explain that it's needed many information from various viewpoint of a networked system so the vulnerable thread and problem can be identified. Protection on critical infrastructure require to fulfill protection standards and principles meet security, safety and compliance goals, alleviate risk and control costs and funds at the same time providing physical protection to critical equipment should always be part of the plan on organization to protect their critical infrastructure properly (Sinisi, 2016).

3. Historical attack on Muslim worlds

Based on Muslim Countries experience, the following examples from websites and other different public sources demonstrate that a broad array of information and assets remain at risk. Several unexpected malware attacks in various Muslim countries took place in the past few years. Such attacks did not require high level of proficiency since they were in countries with old mentality, in cybersecurity of course, where they still anticipate the thefts to use traditional techniques such as blowing the torches using oxy-acetylene to open cash compartment of a certain machine or to invade public sector facilities using machine guns. Despite of the IT infrastructures that some countries such as Malaysia, Turkey and UAE have, the security measures are still primitives compared to countries that have the same level of infrastructures. Malaysia has suffered from hacktivists intrusion recently. The worst hacking operation was when a Latin American gang made off over RM3 million by hacking into fourteen different bank branches belonging to Bank Islam (infosecinstitute, 2015), Al Rajhi Bank and Affin Bank. He easily took advantage of the obsolete ATM's system (Windows XP) and used a known malware "ulssm.exe" to furtively hack into the vulnerable ATMs. The suspects opened the top panel of the ATM machine without using any key and immediately inserted a compact disc into the processing centre of the machine (www.arabnews.com, 2015). Accordingly, the ATM's system rebooted. The erudite gang then used a keyboard to subtly hack into the ATM's system and take out money. However, using such method can result in taking out up to 40 notes in a single transaction. He used a computer malware known as "ulssm.exe" to hack into the ATMs. The sophisticated gang then used a keyboard to hack into the system and take out money. Up to 40 notes could be taken out in a single transaction using the method. In such case of ATM's thefts, the hackers could most probably infect their CD with "Backdoor.Padpin" Trojan horse. As soon as the compact disc is inserted, the ATM system reboots and executes this type of Trojan horse that creates "[PATH TO THREAT]\ulssm.exe" file (rawangpost, 2014). They ignored erasing, or forgot to erase, the Trojan horse from the ATM which unveiled the operation to the authorities. Nevertheless, this is not the first hacking attempt in Malaysia. Back to the year 2000 when Malaysia's national budget speech document on the official website of the Ministry of Finance was infected by malware that might overwrite and edit the Microsoft Word document with entering some rude comments against the Malaysian Prime Minister at that time (Mahathir Mohamed). Saudi Arabia is amongst the Muslim countries that survive several malicious malware attacks. The hacktivists attacks in Saudi Arabia are distinctive to some extent due to the diversity of hacked targets and the reasons behind these malware acts. Most attacks were intended to hack the government websites for some political reasons, either by antagonistic governments or by human right activists. The attacks for this cause accounts for 39% of overall breaches (rawangpost, 2014). The media has its share of attacks for the same reason as the government websites with a percentage of 23. Then come the cyberattacks on the telecoms and Information Technology sector, and on the utilities websites with a percentage of 15 and 8 respectively. The hackers accessed different websites in the country through email proxies. The process flew smoothly from the commencement of gathering the information on battered websites and their directorates going through decoding passwords to uploading fishing files. Fortunately, the government detected these breaches and alerted the targeted sectors as well as their directorates. However, one of these malware infringements was about to cause a fatal damage to the financial system of Aramco (the giant oil firm) when more than 30,000 workstations were hit by cyberattack on 15th August 2012 during the holiday of the holy month of Ramadan. Such breach is deemed to be the worst in the world as it was intended to hack the most effective company in the world of oil exploration. Cutting Swords of Justice was the unknown group who claimed the responsibility for this attack. Neither the hackers nor the firm experts mentioned the name of the malware. However, security researchers indicated that the Shamoon malware was used (BBC, 2012). Such malware has the capability to both over-write data and to damage Master Boot record files which makes the infected Windows machines impossible to boot. The over-written files were placed by US flag in the shape of a burning image. The only instant protection available against this attack was a decision to suspend the firm website for a few days which, this feeble precaution, can create a loss to some extent as the remote access to services was suspended. Fortunately, the primary exploration and production systems were not affected, but we do not have intuition what might happen in the coming hacking attempts as the only future precaution from the firm is a promise to upgrade the security system. The hackers anonymously also conducted a DDoS swift breach on the website of Saudi Arabia Ministry of Defense which result in compelling the website to be offline for more than a day (Amir, 2015).

4. Cyber Security Challenges

Todays, Attackers have become more creative, reaching corporate resources with modern and complex malware attacks. Malware meaning software that can be used to compromise computer functions, steal data, bypass access controls, or otherwise cause harm to the host computer. Malware is a broad term that refers to a variety of malicious programs. This post will define several of the most common types of malware; adware, bots, bugs, rootkits, spyware, Trojan horses, viruses, and worms.

4.1 Infecting malware type

The most attack on Muslims countries come from India, USA, and activates in human rights. They attempt to steal important information or destroy infrastructure of ICT in these countries, some of these attacks really harmful in some case maybe shutdown the websites and systems (Clark, 2015). As a result for these damage cost Muslim countries highly amount of money. The common recently attack on Muslim countries as listed below:

4.2 Bot communication

Bot is a malicious software has ability to invade personal computers as well as servers, and it is responsible for a most criminal activities on the internet. The way of Bot communication works is straightforward. Attackers install a network of control over the network or spread it, and steal the computing and communication system resources. Then they sold data for willing buyers who will invest information in many ways to earn money or causing harm (Clark, 2015).

4.3 Access to Malicious Resource

This mechanism use legally by systems administrators for accessing computers in the networks to solving problems can by happened. However hackers get unauthorized access to servers in order of it, they get remotely access or control the systems without knowledge of victims. Most of the popular cybercriminals are capable of performing key logging, screen and camera capture, file access, code execution, registry management, password sniffing etc.

4.4 Malicious file transfer

Pirates in this case attack the channel which use to transfer file between the senders and receivers.

4.5 Others type of attacks

Such as Adware, bug, ransomware, and so on. Some government's websites request uploading files for starting process somethings such as visa, and so on. Computer criminals use this features to upload malicious files to attacking on systems or websites.

5. Recently Attack on Muslim Worlds

Overall, in 2016 the most significant source of attack on UAE, Saudi Arabia Turkey and Malaysia is USA witch together accounted over one-third of cyber-attacks. While India, France and other countries around the world generate the least attacks. The pie charts below illustrate the type of attacks and percentage of each attacks:

5.1 Attacks on UAE

Most frequent attacking country USA (CheckPoint, 2016)
UAE attacked by Bot communication comprised of 49.3% in Nov 2016.likewise access to malicious resource is 27.2%. The third and fourth attack categorizations reported are malicious file transfer and spam with 20% and 3.5% respectively.

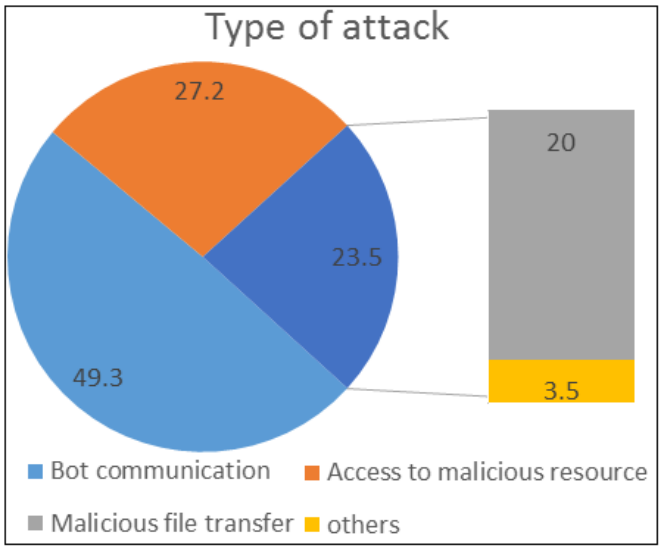

Figure 1: Attacks on UAE (checkpoint)

5.2 Attacks on KSA

Most frequent attacking country is USA. Saudi Arabia attacked by Bot communication comprised of 88% in Nov 2016.likewise access to malicious resource is 27.2%. The second, third and fourth attack categorizations reported are access to malicious resource, malicious file transfer and spam with 7%, 4% and 1% respectively.

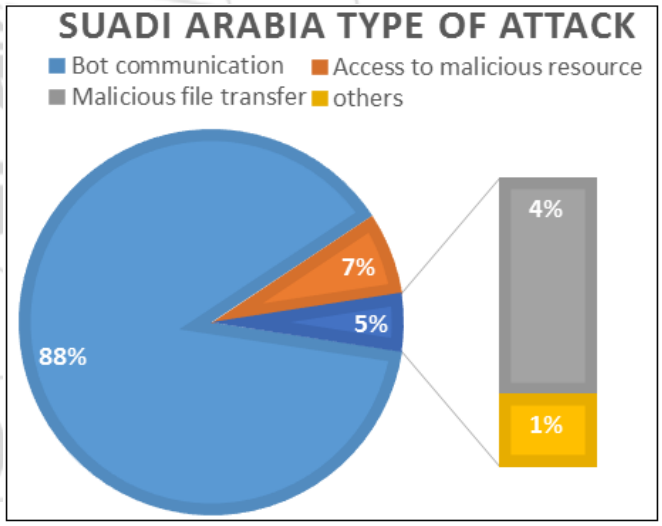

Figure 2: Attacks on KSA (checkpoint)

5.3 Attacks on Turkey

Most frequent attacking country is France. Turkey attacked by Bot communication comprised of 54% in Nov 2016.likewise access to malicious resource is 29%. The third and fourth attack categorizations reported are malicious file transfer and spam with 14% and 3% respectively.

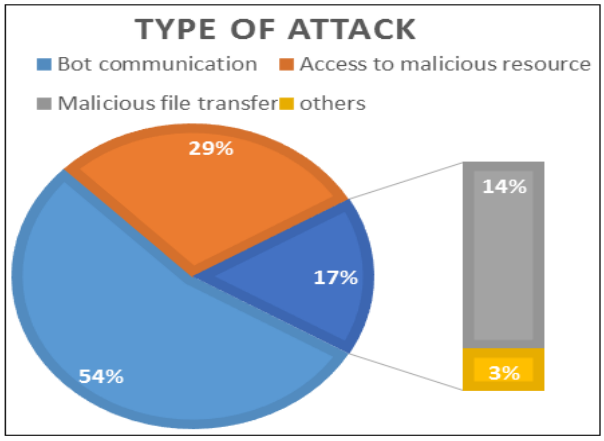

Figure 3: Attacks on Turkey (checkpoint)

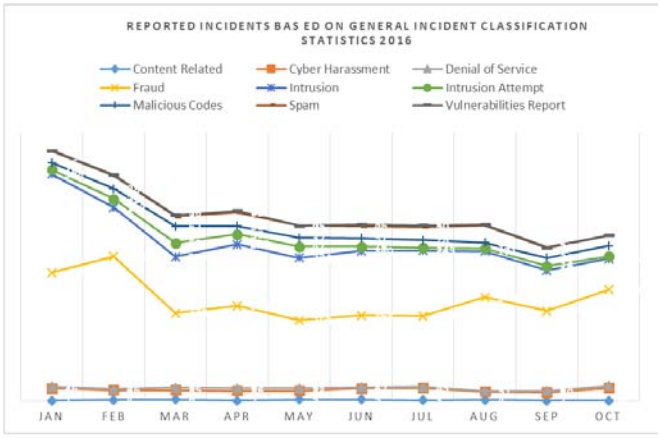

Figure 5: Classification Statistics 2016(MYCERT)

5.4 Attacks on Malaysia

Most frequent attacking country is Netherland and France. Malaysia attacked by Bot communication comprised of 57% in Nov 2016.likewise access to malicious resource is 23%. The third and fourth attack categorizations reported are malicious file transfer and spam with 15% and 5% respectively.

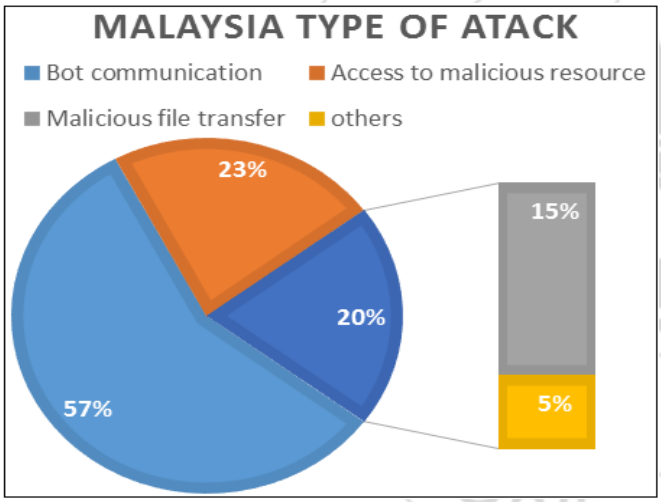

Figure 4: Attacks on Malaysia (checkpoint)

6. Malware threats (Malaysia Case Study)

The graph in figure 5 highlights the activities accomplished by the Malaysia Computer Emergency Response Team, a department responsible for Cybersecurity in Malaysia. These activities are concerning to computer security incidents and directions based on security incidents handled by MyCERT (MyCERT, 2016).

A total of 3295 fraud incidents were received from the beginning of 2016 to October, from organizations and home users. Frauds incidents are first most reported incidents which represents 47.13% of the total reported incidents to MyCERT. By analyzing the current situation and see the trend, it is expected to increase fraud incident over the time. As a result of that, MyCERT urges the Internet users to take caution and always to deal trusted websites when selling goods online.

Other advice is "Do not" pay money before ensuring that the dealing is made with trusted parties. The second incident categorization reported is intrusion with 30%. The third and fourth incident categorizations reported are cyber harassment and spam with 6.68% and 5.46% respectively.

7. Analysis and Solutions

It can be noticed from the nature of malware attacks in each of the discussed countries that the hacktivist either targeted the financial systems or some salient sectors such as the military facilities. The hacktivists in Malaysia hacked the financial systems including banking and the ministry of finance. On the other hand, the type of attacks in Turkey and Saudi Arabia had political concerns. Consequently, the suggested solutions will vary regarding to the type of targeted sectors whether it's economical or more secret such as political systems and military facilities.

We propose two crucial solutions: one with economical basis that some countries will benefit from such as Malaysia and UAE. We will take Malaysia as an example where the sense of security in the financial system draws more concerns since it has one of the prominent and growing financial systems in eastern countries; and the other solution will bear more discrete concerns as the situation of KSA and Turkey. The more reliable and straightforward solution will be the one with economical prospective as it's not intricate. The governments of such type of hacktivist can benefit from the experience of the other nations that have the precedence in cybersecurity. Therefore, taking advantage of countries with advanced technology will be the appropriate solution in the short term for the situation in Malaysia. Then, according to Malaysian government plans, the cybersecurity sector will be fully improved by the year 2020.

On the contrary, the countries the hackers targeted its military and sectors with more privacy as the political systems and the power industries, such as in Turkey. The assistance of other nations is impossible, because such countries have their own enemies and eliciting support might bring harm as the trustworthiness between different nations in the military information is ceased to exist. That means, Turkish and Saudi governments are still between a rock and a hard place as they are still subjected to hackers, or if they

decide to benefit from other countries experience in internet security which may lead to spying on the most salient information of the government. Thus, the only appropriate solution for them, Turkey and Saudi, is to start developing their own technology. Turkey might be able to enhance its systems, but not in the near future. Saudi Arabia seems to lack the serious research in information security. However, in the meantime, they are still behind in this technological advancement. Therefore, the most suitable approach to tackle such issue would be the extensive cooperation between all Muslim countries, especially, those who have technology, or at least they have the capabilities to provide such technology from one side; and the countries that need the cybersecurity technology and they have excessive amount of money, from the other side, such as Saudi Arabia and UAE. Because, as we all know that some Muslim Countries are in good financial condition, so that they can provide all financial support needed. Some Muslim countries, on the other hand, have the human power and the research facilities as well as the experience in technology, but they lack the proper source of money to maintain and cultivate the research in this technological field. Hence, the collaboration between all countries will be complementary. By such cooperation, the Muslim countries will be on the right path through acquiring high level of cybersecurity technology.

8. Evaluation

We have perceived that, despite of the frequent hacking attacks, the governments are still in the same level of security with no distinctive further upgrades which can be recognized by the same methods the hacktivist recurrently use. Therefore, the governments of the aforementioned countries shall be taking immediate and serious precautionary measures. Otherwise, there might be more severe attacks in the future due to the rapid improvement of technology and the new means the hackers use in response to this improvement. Muslims countries also have to share information and create one platform for working on it to achieve the desire results and protect their infrastructure such as preparing framework to test mutuality across the community and information sharing machineries which could be used in some ways. Then Discuss cyber information sharing issues from all Muslim countries. And Information sharing is serious for well-timed reaction to cyber actions that can have a wasteful impact in seconds.

9. Conclusion

It can be perceived that, despite of the frequent hacking attacks, the governments are still in the same level of security with no distinctive further upgrades which can be recognized by the same methods the hacktivist recurrently use. Therefore, the governments of the aforementioned countries shall be taking immediate and serious precautionary measures. Otherwise, there might be more severe attacks in the future due to the rapid improvement of technology and the new means the hackers use in response to this improvement which means that these countries will be turned into a quagmire if they do not perform a myriad of reformations.

References

[1] Amir, W. (2015). DDoS Attack Shuts Down Saudi Ministry of Defense Website. hackread.com Web.
[2] Ashraf, G. (2015). Cyber terrorrism threats. New York: Utica College.
[3] BBC. (2012). Saudi Aramco says most damage from computer attack fixed. BBC 26.
[4] CheckPoint. (2016). ThreatPortal/livemap. CheckPoint.
[5] Clark, R. M. (2015). Protecting Critical Infrastructure. Springer International Publishing Switzerland.
[6] Fischer, F. e. (2013). Grand challenges in technology enhanced learning Springer.
[7] Gouglidis, B. Green, J. Busby, M. Rouncefield, D. Hutchison and S. Schauer. (2016). Threat awareness for critical infrastructures resilience. 8th International Workshop on Resilient Networks Design and Modeling (RNDM), 196-202.
[8] Infosecinstitute. (2015). Hacking ATMs: The new wave of Malware. Infosecinstitute.
[9] MyCERT. (2016). Incident Statistics as of October 2016. . MyCERT.
[10] Rawangpost. (2014). Here's How Malaysian ATMs Were Hacked of RM3 Million by Latin Americans. www.rawangpost.com.
[11] Shwani, H. G. (2014). CRITICAL INFRUSTRUCTURE PROTECTION. Utica College: ProQuest LLC.
[12] Sinisi, J. P. (2016). CRITICAL INFRASTRUCTURE PROTECTION FOR SUBSTATIONS AND TRANSFORMERS. IEEE Symposium on Technologies for Homeland Security (HST), 1-6.
[13] Watts, R. (2005). Maritime Critical Infrastructure Protection: Multi-Agency Command and Control in an Asymmetric Environment. Homeland Security Affairs, 1-3.
[14] www.arabnews.com. (2015). Bank account of Saudi hacked. Arabnews.
[15] Xiaoxue Liu, Jiexin Zhang, Peidong Zhu. (2016). Dependence Analysis based Cyber-Physical Security Assessment for Critical. 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 1-7.

Author Profile

Sami Mohammed Abdulrahman Ali, Master of Information Technology, Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia

Muhammad Abdu, Master of Information Technology, Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia.

Jamaludin Ibrahim, Academic Fellow, Department of Information Systems, Kulliyyah of Information and Communications Technology, International Islamic University Malaysia.