Cyber Threats Early Detection Countermesures and Benefits

Husam Hassan Ambusaidi

Department of Postgraduate Studies and Consultancy
Middle East College
Muscat, Oman
PG15F1547@mec.edu.om
Dr Prakash Kumar Email ID: (Prakash@mec.edu.om)

***Abstract*— In the recent years, the cyber-attacks have evolved and become more complex. The cyber-attacks have moved from random attacks to targeted and high sophisticated attacks. On a daily basis, companies and organizations are targeted by different and sophisticated cyber attacks. Many of these companies and organizations are unconscious that they are targeted by cyber threats and their networks are already compromised. Furthermore, vast majority of companies and organizations are vulnerable to various cyber threats. Hence, to detect the cyber threats and compromised networks at early stage the organizations need better mechanism for cyber threat detection. Several cyber security vendors have introduced advanced technologies to allow early detection of the cyber threats. This research will discuss the importance of early detection for cyber threats. Furthermore, the research study the current emerged cyber threats with relation to early detection. Further outcome, this paper research will identify the benefits of proactive security protection.**

Keywords—Threat; Cyber; Attacks; proactive security; security feeds, Malware; Viruses; Wormsv

I. INTRODUCTION

At the present time, information technology become an important player in every aspect of our life. The valuable data is flowing through the internets and networks all around which makes our life better.

In the other hand, the data and information systems carrying this data become valuable target for criminals, business competitors, and even state sponsored espionage groups. Hence, the protection the data and information systems became a hard work for IT security professionals and experts. The important data which requires protection from various cyber threats can be found in different information systems such as financing systems, internet of things systems, health sector systems, airports systems, and water and electricity systems. As the number of information systems increases, the cyber threats targeting these systems increasing. In the recent years, Information systems and the data which carry has been targeted by countless cyber-attacks. Companies and organizations suffered from highly sophisticated cyber-attacks which causes huge financial and reputational impacts. Hence, to allow better and proactive actions against these cyber-attacks, the cyber security vendors have introduced technologies to allow early detection for cyber threats and attacks. First of all, let us understand to meaning of cyber threats. According to the Federal Information Processing Standards Publication, the cyber threats is any incident or condtion with the chance to harmfully affect organizational work or operations such as functions, tasks, reputation, properties, or entities over an IT system through unauthorized access, leak, destruction, modification of data, or denial of service. Furthermore, the likely for a threat to effectively exploit a specific information system weakness, flow or vulnerability [10]. The Cyber security company Symantec published report shows that in 2016 approximately 229,000 is the average number of web cyber-attacks detected in daily basis by the company around the world [2]. By the appropriate solutions most of cyber-attacks can be detected proactively.

II. CYBER THREATS DETECTION

Due to the revolution of information systems and technologies, the detection of cyber threats become tough task. Detecting the threats over the cyber space and networks is critical for every business IT security strategies and plans. Moreover, detecting the threats at earlier stage is better than recovering

from successful cyber-attacks. Hence, to allow the earlier detection IT security companies introduced many solutions such as Cyber Threat Intelligence (CTI) platforms, Anti DDoS solutions, and cloud based sand box.

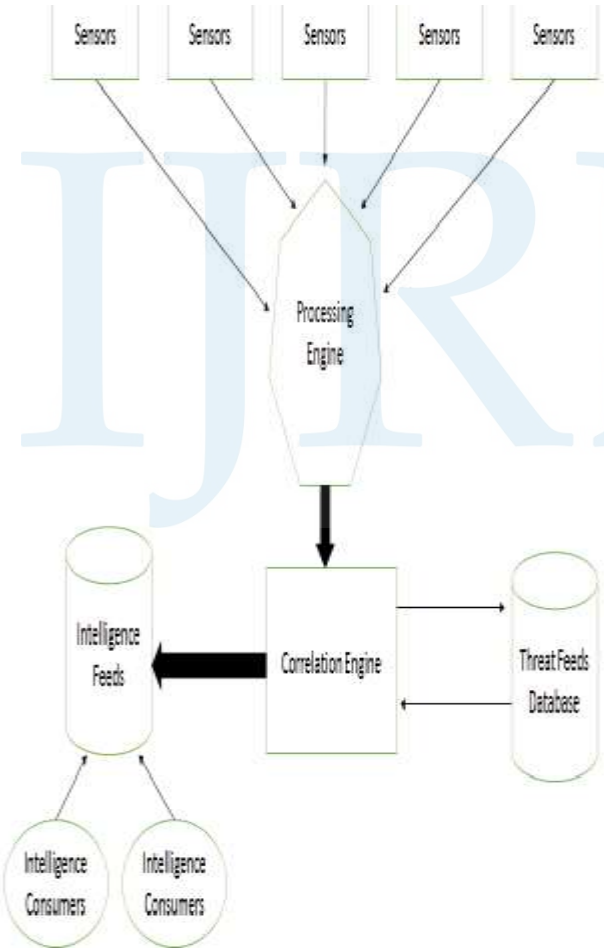
A. Cyber Threat Intelligence (CTI) Platforms

Cyber threat intelligence platforms are solutions that provide IT security feed sharing in organized, faster, and reliable mechanism. Many of popular IT security companies provides Cyber Threat Intelligence platforms as well as the open source platforms. Platforms such as iSIGHT, Deep Sight, TALOS, Open Source Intelligence (OSINT).

Cyber threat intelligence platforms provide wide, broad threat intelligence across all classifications of threats such as (cyber-crime, critical infrastructure, hacktivism, cyber espionage, and much more). CTI platforms brings visibility over an extended cyber-attacks life cycle based on an unmatched view across attackers, victims, and networks around the world [5]. In addition, CTI platforms extends the support to five major cyber security areas threat intelligence, detection research, vulnerability research and outreach, engine development, and development. Moreover, CTI platforms analyze the cyber threats across web, networks, cloud environments, emails, and end points. After analyzing these threats, CTI platforms share a complete understanding of cyber threats, scopes of outbreaks, and their root causes with its customers. CTI platforms are automated solutions which continuously detecting and searching for new cyber threats. When new threats are discovered, CTI platforms releases advisories and rules to protect against these threats. By providing such information, the possibility to response to such threats proactively is increased [3].

Cyber threat Intelligence platforms grant customers with relevant, timely, reliable intelligence information regarding emerging threats, threat sources and vulnerabilities to enable incident response teams to keep up-to-date with the changing threat. For example, the DeepSight platform collects information from more than 240,000 sensor monitoring different networks in more than 200 countries around the world, more than 133,000,000 Symantec technology products and services, visibility into all internet ports/protocols for threat collection and analysis, over 8 billion emails tested per day, and over 1 billion web requests daily [4]. By having large number of sensors and information gathering agents, CTI platforms allow better and broad threat intelligence from different sources. CTI platforms grant the customers the advantage of timely and reliable threats information with suitable countermeasures.

Fig. 1. CTI platforms mechanism



Through the CTI platforms customers have the advantage of cyber threats knowledge. In addition, customers can get information about vulnerabilities, IP addresses, and code signatures which may be used to conduct future cyber-attacks.

The CTI platforms provides the vulnerability intelligence which is threat intelligence service provide timely and different critical vulnerabilities information from different technology vendors. Moreover, using such intelligence information allows quick vulnerabilities patching and bug fixes. Furthermore, this mechanism stops attackers from utilizing the vulnerabilities that are exist in the information systems as it allows fast patching and fixes [9]. Another feature of CTI

platforms is the malware codes/signatures Intelligence. This feature uses the sensors that installed around the globe, threat intelligence platforms providers gather information about new sophisticated malwares, Trojans, viruses, and worms. After collecting the intelligence, the analysis of malicious codes will take place. Then signatures and codes of these malicious codes will be shared among customers to allow better and prior prevention against these malicious codes [6] [11]. The black listed IP addresses /domains and URLs intelligence is a type of cyber threat intelligence which monitors the Internet Addresses (IPs), malicious domains, and URLs that are malicious or used to conduct malicious activities [8]. After collecting the threats information about IPs and domains, the intelligence information will be progressed to the customers to enable them to do better detection and prevention.

B. *Anti DDoS solutions*

Stopping the Distributed Denial of Service (DDoS) attacks is very complex task. Furthermore, all available countermeasures in the market didn't prove high percentage of effectiveness. Some IT security companies such as Arbors Networks has presented anti DDoS protection solution. Anti DDoS solutions integrates different technologies such as cyber threat intelligence platforms and anomaly detection to detect DDoS attacks. In addition, Anti DDoS solutions uses cyber threat intelligence to detect the malicious IP addresses lists to detect then block any DDoS attacks. Moreover, Anti DDoS solutions integrate the client's solutions with Internet Service Provider (ISP) to block the incoming attacks from prior level. Anti DDoS also uses anomaly detection mechanism to detect any malicious traffic. The anti DDoS solution analyzes the nature of the traffic and also the range of IP addresses to detect any suspicious traffic [12].

Anti DDoS solutions combines multiple cyber threats detection technologies such as anomaly detection, IP addresses reputation services, and traffic analysis.

III. CYBER INCIDENT RESPONS AND THREAT DETECTION

Cyber incidents response and threat detection need to be aligned together for better and earlier protection. Moreover, if any cyber incident occurred, incident responds teams must follow several

procedures to manage the incident. Incident management life cycle has four major phases are Prevention, Detection, Response, and Reporting.

Fig. 2. Incident Response Management life Cycle

Incident response detection phase is the first and the most critical task to react to threats. In the detection phase of incident response management life cycle, incident response teams need appropriate and accurate information regarding cyber threats that they face. Hence, if the detection phase is failed to provide the accurate information, the likelihood to be attacked will be high. By providing sufficient information in the detection phase, the cyber incident response will be more effective due to different aspects such as timing, accuracy, and relevance. Moreover, the intelligence information feeds about emerging cyber threats with consideration to the timing to allow prior prevention and detection. The accuracy will allow incident responds teams to know the exact threat and its characteristics and behavior. The relevancy allows the incident responders to know the effect of these threats and what the suitable countermeasures [7].

IV. THE IMPORTANCE OF THREAT EARLY DETECTION

The cyber space is full of cyber threats that may well affect any organization at any time. Cyber threat detection should be an important part in every organization incident response plan and overall IT security strategy. Furthermore, by investing and focusing in the threat detection, organizations and companies can avoid many cyber threats. The importance of cyber threats early detection can be summarized in the below points:

- The earlier detection gives the security teams the chance to contend the threats before the attacks.
- Earlier detection allows quicker protection against emerging threats in the cyber space
- The detection of undiscovered security breaches and malware infections will be easier and more accurate.
- Sufficient threat information allows the automation of incident response using smart response.
- Give the organization better monitoring view to their networks.
- Proactive protection will save the organizations in terms of cost and reputation in case of successful cyber-attacks.
- Early detection then prevention can protect the organizations from future cyber attacks

V. CONCLUSION

This paper has explored the different cyber threats early detection countermeasures. Furthermore, the paper also addressed the outlined the importance of cyber threats early detection. The outcome of this paper is identifying the benefits of cyber threats early detection. The paper assessed the need for threat detection solutions to contend cyber threats. In conclusion, cyber security is rapid changing field were the experts, professionals, and IT security service providers need to be innovative and up to date to be aligned with emerging cyber threats.

References

[1] Threat Connect, "THREAT INTELLIGENCE PLATFORMS Everything You've Ever Wanted to Know But Didn't Know to Ask", Threat Connect, Arlington, 2015.

[2] Symantec, "Internet Security Threat Report", 2017.

[3] *TALOS Group*, 1st ed. TALOS Intelligence, 2016, pp. 2-4.

[4] *Symantec DeepSight Security Intelligence Solutions*, 1st ed. Symantec, 2012, p. 1.

[5] FIREEYE ISIGHT THREAT INTELLIGENCE SCALABLE THREAT INTELLIGENCE FOR ADDED CONTEXT ACROSS THE ORGANIZATION, 1st ed. FIREEYE, 2016, pp. 1-3.

[6] E.M. Hutchins, M.J. Cloppert and R.M Amin PH.D., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proc. 6th Int'l Conf. Information Warfare and Security (ICIW 11), Academic Conferences Ltd., 2010, pp. 113–125;

[7] AMIN,R.M.,RYAN,J.,H,J.C.,AND VAN DORP,J.R. De-tecting Targeted Malicious Email. IEEE Security & Privacy 10,3(2012),64–71.

[8] J. Jose, J. Jose, F. Jose, "A survey on secure data aggregation protocols in wireless sensor networks", *International Journal of Computer Applications*, vol. 55, pp. 17-21, October 2012.

[9] B. Koldehofe, F. Dürr, M. A. Tariq, K. Rothermel, "The power of software-defined networking: Line-rate content-based routing using openflow", *Proceedings of the 7th Workshop on Middleware for Next Generation Internet Computing*, ACM, pp. 3:1-3:6, 2012.

[10] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION (2006) Minimum Security Requirements For Federal Information And Information Systems, 2006

[11] Robinson N., Gribbon L., Horvath V, Robertson K., *"Cyber-security threat characterization A rapid comparative analysis," 5-6(2013).*

[12] David Karig, Ruby Lee, *Remote Denial of Service Attacks and Countermeasures,*: Princeton University Department of Electrical Engineering Technical Report CEL2001-002, (2001)