International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 3 Issue 5, August 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Information Sharing of Cyber Threat Intelligence with their Issue and Challenges

Khin Myat Nwe Win, Yin Myo Kay Khine Thaw

Lecturer, Faculty of Computer Science Department, University of Computer Studies, Mandalay, Myanmar

How to cite this paper: Khin Myat Nwe Win | Yin Myo Kay Khine Thaw "Information Sharing of Cyber Threat Intelligence with their Issue and Challenges" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-5, August 2019, pp.878-880, **https://doi.org/10.31142/ijtsrd26504**

IJTSRD26504

ABSTRACT

Today threat landscape growing at the rapid rate with much organization continuously face complex and malicious cyber threats. In today's Internet-connected world where technologies support almost every feature of our society, cyber security and forensic specialists are increasingly distributing with wide-ranging cyber threats in almost. real-time conditions. The capability to detect, analyze, and defend against such threats in near real-time conditions is not possible without the employment of threat intelligence, big data, and machine learning techniques. Cyber Threat Intelligence (CTI) has become a hot topic and being under consideration for many organizations to counter the rise of cyber-attacks. The vast majority of information security challenges we face today are the result of serendipitous and naive decisions made in the early stages of the Internet.

KEYWORDS: *cyber security, threat intelligence, threat*

I. INTRODUCTION

Cyber threat intelligence (CTI) is an area of **cyber security** that focuses on the collection and analysis of information about current and potential attacks that threaten the safety of an organization or its assets. [1] Cyber security are the techniques of protecting computers, networks, programs and data from unauthorized access or cyberattacks that are aimed for exploitation [3]. The benefit of threat intelligence is that it's a proactive security measure, preventing data breaches and saving you the financial costs of cleaning up after an incident.

Threat intelligence is the analysis of internal and external **threats** to an organization in a systematic way. Cyber Threat Intelligence (CTI) can still be described as a nascent and fast-developing field. However, the practice of intelligence itself is historically and commercially a very well-established discipline. Cyber Threat Intelligence (CTI) can still be described as a nascent and fast-developing field. [2]. The security community has produced a cluster of promising intelligent based cyber security collaborative research with particular focus on gathering, sharing and analytics of cyber threat intelligence. From the perspective of cyber security, there act to be interoperability issues and disconnection between research and development frameworks, business organizations' attitudes towards security, and the research strategies put in place. It is important for the information security community to understand the basic concept to define cyber threat intelligence and how it is derived. As a starting point, this paper will begin the definition of cyber security intelligence and then described the different level of cyber security intelligence and threat intelligence provider. that always being used extensively and interchangeably by the security community in threat intelligence.

II. CYBER SECURITY INTELLIGENCE

In **Cyber-Threats and Cyber-Attacks**, there is no agreement between the security community on how to clearly define cyber-attack and cyber-threat while this term is used interchangeably. In [6], start analyzing CTI definition for this paper by considering cyber-attack and cyber-threat because it is a basic building block in all hostile cyber situation. There are many definitions to clarify cyber-attack and cyber-threat as both terms being the most discussed issue in mainstream media. In 2013, the US Government defined cyber-threat as a broad definition that covers a wide range of security measures: It is stated that cyber-threats cover a wide range of malicious activities that can occur through cyberspace. Such threats include web site defacement, espionage, theft of intellectual property, denial of service attacks, and destructive malware. In contrast to US Government, the Oxford English Dictionary defines cyber-threat, "as the possibility of malicious attempts to damage or disrupt a computer network or system". While cyber-attack is "an attempt by hackers to damage or destroy a computer network or system". This definition gave us an insight that cyber-threats are the condition when there is a possibility of malicious activity happens and cyber-attacks are when the incident becomes reality.

Cyber Threat Intelligence (CTI) can be defined comprehensively as evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging threat that can be used to inform decisions regarding the subject's response to that menace or hazard [7]. As threat landscape evolve and grow more sophisticated, there is still no general agreement to define cyber threat intelligence with information security community often incorrectly using the terms intelligence,

cyber intelligence and cyber threat intelligence [5]. In [6] proposed, cyber threat intelligence is important for the information security community to understand the basic concept to define cyber threat intelligence and how it is derived. We decide to cover four relevant terms in this field: cyber-attack, cyber-threat, intelligence and cyber threat intelligence.

In **Cyber Threat Intelligence (CTI) Sharing,** the success of any cyber security strategy is proportional to the amount of rich and cyber threat intelligence available for analysis and the speed intrusions are detected and blocked. In the process of refining security practices, worldwide cyber security centers, vendors, manufacturers, and institutions have gathered, compiled, and produced humongous amounts of cyber threat information. Currently, cyber threat analysts have at their disposal intelligence produced and maintained by a wide range of sources including cyber security research and information centers, information security companies, technical reports and post mortems, ontologies and vocabularies, reference models, knowledge bases, databases, system and application logs. Some of this cyber threat intelligence is made freely available but unfortunately unstructured, formatted differently and not easy to access. This is problematic, particularly in the sharing of evidence-based knowledge about advanced persistent threats, assets risk assessment, adversary strategies, security best practices, and decision-making problem is not the lack of intelligence but the lack of interoperable standard frameworks for information sharing and big data analytics. [8]

III. DIFFERENT LEVELS OF CYBER THREAT INTELLIGENCE

There are different levels of cyber threat intelligence: operational, tactical, and strategic.

Operational threat intelligence often relates to details of potential impending operations against an organization. Operational intelligence is knowledge gained from examining details from known attacks. An analyst can build a solid picture of actor methodology by piecing together tactical indicators and artifacts, and derive into operational intelligence Although it is not always easy to obtain, by using an all-source approach an intelligence provider will be able to detect, for example, chatter from cyber activists discussing potential targets for an upcoming campaign, or data leaked or sold on a dark web forum that could be used in an operation against the company. Cyber threat intelligence providers will generally supply operational threat intelligence in a combination of human and machine-readable formats.

Tactical threat intelligence consists of material relating to the techniques, tactics and procedures (TTP's) used by threat actors. Indicators of compromise (IOCs) are the main deliverable for tactical threat intelligence providers. These are particularly useful for updating signature-based defense systems to defend against known attack types, but can also prove useful for more proactive measures, such as threat hunting exercises. It is therefore particularly useful to network defenders such as Security Operations Centers (SOCs). CTI providers will generally supply IOCs in machine-readable formats, whereas intelligence on TTP will be in human-readable formats, and will require human assimilation and action.

Strategic threat intelligence exists to inform senior decision-makers of broader changes in the threat landscape. Because of this intended audience, strategic intelligence products are expressed in plain language and focus on issues of business risk rather than technical terminology. The reporting format of strategic cyber threat intelligence products will reflect this longer-term view – for example it will often be disseminated on a monthly or quarterly basis to assist the formulation of a longer-term strategy. [1]

Fig (1) the three levels of cyber threat intelligence

IV. CYBER THREAT INTELLIGENCE PROVIDERS

Threat intelligence providers then utilize this data to provide businesses with the most relevant information in order to help them prioritize security measures and stay cognizant of the viruses, scams, and other trends in cybercrime. Threat intelligence services go hand in hand with cyber security consulting, incident response, and other cyber security services to keep companies aware of threats, safe from attacks, and prepared to respond in the event of a breach or related event. Businesses can deploy threat intelligence software in lieu of or in addition to threat intelligence services in order to maximize awareness and protection. There are two tools that can be used for nomenclature and dictionary, Common Platform Enumeration (CPE) for hardware and Common Configuration Enumeration (CCE) for security software configurations.

Here are some examples of threat intelligence companies:
FireEye, this is one of the industry leaders in threat intelligence and cyber security in general. It targets large enterprises and provides nation-state-grade threat intelligence and cyber security consultation. Consider this company if you're in a business that deals with highly sensitive information, such as government secret services, financial institutions, healthcare companies and other businesses that are willing to pay out large sums of money for the absolute best in the industry.

IBM X-Force, most people know IBM for its hardware products, but the company has also developed a strong threat intelligence program. IBM X-Force is the world-renowned threat intelligence program that allows users to research threats and collaborate with peers through a cloud-based threat intelligence sharing platform. Like FireEye, it is tailored to larger companies that need a comprehensive intelligence program.

Threat Tracer is a threat intelligence company tailored to small and midsize businesses. It provides cyber security solutions for companies that don't have large internal security teams. Firstly, Threat Tracer offers cyber security solutions that automate many of the manual security processes that IT teams to execute. This helps smaller

companies make up for the lack of dedicated manpower when it comes to cyber security. Secondly, through quality threat intelligence, Threat Tracer allows small and midsize companies to focus their limited resources on their most concerning issues. [9]

V. CYBER THREAT INTELLIGENCE ISSUE AND CHALLENGES

With cyber threat intelligence, type of threat data source and threat intelligence sharing platform (TISP) examined, it is crucial to look at the current issue and challenges in cyber threat intelligence area. This section identifies four current issues and challenges facing by consumer and producer of threat intelligence. [6]

Challenge 1: Threat Data Overload Threat intelligence has evolved in a very short period and there are hundreds of threat data feed available whether from open source, closed source or free to use. To defend against cyber-attack, it is very important for the customer to have timely access to relevant, actionable threat intelligence and the ability to act on that intelligence [10]. However, many of them still struggle with an overwhelming amount of threat data and a lack of staff expertise to make the most of their threat intelligence programs.

Challenge 2: Threat Data Quality It is common practice for security feed provider to market threat feeds as CTI. Security feed provider needs to redesign their security sensors to capture and enrich the data to help decision-support systems increase the value of threat intelligence and make it actionable. There is an initiative by Cyber Threat Alliance (CTA) to improve threat intelligence quality that is shared among community members. Threat intelligence coming from CTA members will be automatically scored for its quality, and members will be able to draw out threat intelligence only if they have provided sufficient quality input.

Challenge 3: Privacy and Legal Issue When dealing with CTI, there are privacy and legal issues to consider that relates to how the data can be shared and which laws govern the sharing of data. Many organizations are wary of sharing information that could reflect negatively on their brand [11]. Some companies may be hesitant to share information due to the fear of reputation damage that may arise from disclosing attack information. As for now TISP already provides preliminary functionalities to establish trust between the organizations. However, it is limited to group-based access control and ranking mechanisms.

Challenge 4: Interoperability Issue in TISP Vazquez et al. [12] raised an interoperability issue that faces by existing threat sharing platform. The various standard and format used by threat sharing platform hindered the producer and receiver speak seamlessly to each other due to data extension is not supported by the used application. However, if there is no data standard can be established between peers due to some constraint, data transformation can come in handy. [6]

VI. CONCLUSION

There are several key points that we can get from the existing definition namely context and element of cyber threat intelligence. The complete cyber threat intelligence definition needs to cover these three elements to make sure only relevant threat data collected, analyze and processed in a timely manner and the result can produce actionable intelligence to assist decision making. We also identify several issues and challenges for data quality and cyber threat intelligence sharing.

REFERENCES

[1] Bank of England, "CBEST Intelligence-Led Testing – Understanding Cyber Threat Intelligence Operations" http://www.bankofengland.co.uk/financialstability/fsc/Documents/cbestthreatintelligenceframework.pdf.

[2] Prafula Talera (2010), "Cyber Threats & Challenges in the Real-world", Proceedings from Conference on Cyber Security, "Emerging Cyber Threats & Challenges, (2010)" CII, Confederation of Indian Industry, Chennai.

[3] G.Nikhita Reddy, G.J.Ugander Reddy," A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies".

[4] Edilson Arenas, (2017), "Cyber Threat Intelligence Information Sharing"

[5] White TLP. An introduction to threat intelligence

[6] Md Sahrom Abu, Siti Rahayu Selamat, Aswami Ariffin Robiah Yusof "Cyber Threat Intelligence – Issue and Challenges".Indonesian Journal of Electrical Engineering and Computer Science Vol. 10, No. 1, April 2018.

[7] Li Qiang, Yang Zeming, Liu Baoxu, Jiang Zhengwei YJ. The framework of Cyber Attack Attribution Based on Threat Intelligence. ICST Inst Comput Sci Soc Informatics Telecommun Eng 2017. 2017;190:92–103.

[8] Edilson Arenas (July 2017), "Cyber Threat Intelligence Information Sharing". School of Engineering and Technology CQUniversity, Australia e.arenas@cqu.edu.au.

[9] https://www.businessnewsdaily.com/11141-cyber-threat-intelligence.html

[10] NIST. Guide to Cyber Threat Information Sharing. Vol. 150. 2016

[11] KPMG. Cyber threat intelligence and lessons from law enforcement. 2013.

[12] Vázquez DF, Acosta OP, Spirito C, Brown S, Reid E. Conceptual framework for cyber defense information sharing within trust relationships. Cyber Confl (CYCON), 2012 4th Int Conf. 2012;1–17.