ISBN 978-981-11-3671-9
Proceedings of 2017 the 7th International Workshop on Computer Science and Engineering (WCSE 2017)
Beijing, 25-27 June, 2017, pp. 611-615
doi: 10.18178/wcse.2017.06.106

Overview of Cyber Threat Intelligence

Wei Weimin [1 +], Kong Zhiwei [2] and Zhao Yan [3]

College of Computer Science and Technology, Shanghai University of Electric Power, Shanghai 200090, China

Abstract. Threat intelligence has been one of the hottest topics for the current network security industry, and it is widely regarded as the most powerful weapon in solving security threats. Now, threat intelligence is shifting from theoretical research to practical application. STIX, TAXII and NIST SP 800-150 Draft will be mainly introduced, and the instance description is based on the machine-readable security threat intelligence in STIX format. Enterprises should customize threat intelligence program in accordance with their own environments, which will be helpful in preventing network attacks.

Keywords: Big data; Threat intelligence; intelligence aware; STIX；TAXII；NIST SP 800-150 Draft

1. Introduction

An information security and protection system is primarily confronted with the following plights. First, it is very difficult to identify real attacks from masses of security incidents and the efficiency of traditional security products such as IDS (Intrusion Detection Systems) and SOC (Security Operations Center), etc. is also low. Second, a confirmed security incident cannot be timely and effectively shared and coordinated within the organization. Third, bugs and threat information of security devices with diverse types and from different manufacturers are not universal, which is unbeneficial to maintenance management of large networks. Therefore, we need to pay more attentions to restraints on sabotages before they give rise to severe damages so as to minimize interferences suffered from by our daily work.

Safeguards against threat intelligence mat the actual value-based adversary. As enterprises gradually abandon a conventional protection strategy giving priority to responses and oriented by devices, they turn to a new path of proactive detection and response that can be realized through intelligence led visualization and control step by step. security posture that we are highly familiar with is falling apart [1].

2. Threat Intelligence

2.1. Definition of threat intelligence

There exist many “hot” words related to threat intelligence, such as Security Intelligence, Threat Intelligence, Security Threat Intelligence, Intelligence Aware, Intelligence Driven and Context Aware, etc. Among multiple definitions of threat intelligence [2], that presented by Gartner [3] is cited frequently; and such a definition is given below. Threat intelligence *is evidence-based knowledge, including context, mechanisms,* indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard. iSIGHT [4] defines the cyber threat intelligence as follows. Specific to attackers and their motivations, purposes and techniques, cyber threat intelligence refers to knowledge that has been collected, analyzed and distributed to assist all levels of securities and business staff to protect core assets of their enterprises. Regarding the SANS Institute [5], it is defined as data set that is collected for the purpose of assessment and

[+]Corresponding author. Tel.: + 86-021-35303729.
E-mail address: wwm@shiep.edu.cn.

application, and targeted at security threats, menace, use of malicious software, bugs and harm index. In addition, some scholars also deem that intelligence is thread and threat intelligence is all threads required to restore attacks that have occurred and predict potential attacks [6]. To sum up, threat intelligence as a whole is constituted by two parts. One is threat information, containing attack sources, attack patterns, attack objects and vulnerability information, etc.; the other is defense information, including access control list (ACL) and rule base/strategy library, etc.

2.2. Functions of threat intelligence

Functions of threat intelligence can be analyzed from diverse perspectives [6]. According to individual standpoints, people who surf the internet by network traffic require agent IP (so as to bypass IP limitation), while security defenders need botnet IP (attackers actually have more needs of it). In terms of enterprises, people who are occupied in Web Application Firewall (WAF), scanner and vulnerability management platform are able to exchange vulnerability information, while those engaged in KillerVirus and intrusion detection, or business fraud and network attack and defense, can exchange malicious sample information or IP reputation information respectively. As a result, integration of internal resources (e.g., security components including scanner, WAF, IPS, etc.) and external resources (e.g., open source resource collection and manufacturer resource exchange) can be carried out to create an effect of cooperative defense and perform thorough analysis that can find truly valuable attack events and advanced APT point attack events indiscoverable.

Common cyber security threat intelligence service listing includes hacker or fraud group penetration, social media and open source information monitoring, directed bug research, in-depth customized manual analysis, technical indicator upgrading, network behavior portal, real-time temporal notice, brand monitoring and protection, credential restoration, fault survey, phishing off line, fraudulent trading correction and notification, and forged domain name detection, etc..

Threat intelligence productization roughly has two directions. Firstly, it is involved with threat intelligence information provision. In detail, one is traditional security product, such as plug-ins including WAF, Anti-malware, DDoS (Distributed Denial of Service), CC (Command & Control), DNS (Domain Name System), SIEM (Security Information and Event Management), SOC and IPS (Intrusion Prevention System), etc.; the other is the enterprise integration solution product that use enterprises as target users, data analysis techniques as supports, and threat intelligence extraction as the objective. Secondly, direction of threat intelligence information exchange is a mainstream profits-earning model overseas at present.

2.3. Status quo of threat intelligence

In recent years, the concept of threat intelligence sharing gradually becomes popular in security domain; in addition, more and more enterprises and countries also begin to pay attention to threat intelligence and study how to employ threat intelligence sharing to effectively defend cyber-attacks. In America, a series of acts and presidential proclamations have been released successively [2]. To be specific, they cover the Network Security Improvement of Key Infrastructure, the White House Executive Orders EO-13636 released in 2013, the Security and Restoring Force of Key Infrastructure, the United States Order No. 21 (PPD-21) released in 2013, the Cyber Intelligence Sharing and Protecting Act (No. 2012CISPA), and the Network Security Intelligence Sharing Act (No. 2015CISA). All these decrees lay foundations for researches on cyber threat intelligence. In America, National Cyber Security and Communications Integration Center (NCCIC) is the major organ subordinate to the Department of Homeland Security (DHS) and it takes responsibilities to promote cyber threat information sharing between government and enterprises. As for the Cyber Threat Intelligence Integration Centre (the CTIIC) under the direct jurisdiction of Office Of the Director Of National Intelligence (ODNI), it is in charge of analyzing and integrating cyber threat information collected by the DHS, FBI, CIA and NSA, etc..

Domestically, the Fenghuotai CTI Alliance [7] was established in October 2015. At present, it has 9 member companies. Not only have lightweight lot-sizing IOC exchange standard and API intelligence interactive mode been constructed, but smooth circulations of secure fundamental data and intelligence have been preliminarily realized within the alliance. In comparison, the Tianji Threat Intelligence Platform [8] is

dedicated to providing the most comprehensive security threat intelligence analysis, inquiry, sharing and visualized correlation services; among which, the Alice CTI Sharing & APT Identifying Platform is quite a special [9]. Currently, threat intelligence is one of the hottest topics in network security industry, the favorable weapon that has been recognized within the industry and can be utilized to solve new security threats. Moreover, it is developing from theoretical research to application practice [10].

Intelligence exchange requires unified exchange standards and the relevant primary standards and organizations consist of STIX (Structured Threat Information eXpression), TAXII (Trusted Automated eXchange of Indicator Information), CybOX (Cyber Observable eXpression), MAEC (Malware Attribute Enumeration and Characterization), OpenIOC (Open sourced schema from Mandiant), IODEF (Incident Object Description Exchange Format), CIF (Collective Intelligence Framework) and IDXWG (Incident Data eXchange Working Group), etc.. Among them, STIX is more popular. As for more information related, please refer to codes and standards associated with threat intelligence sharing[11,12]. This paper focuses on introductions to STIX, TAXII and NIST SP 800-150 Draft.

3. STIX

The Structured Threat Information eXpression (STIX) is proposed in MITRE in its White Paper Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression [13]. Such architecture has been applied into US-CERT. STIX is mainly appropriate for the following four scenes. 1) Threat Analysis. Threats are judged, analyzed and investigated; record keeping is utilized, etc.; 2) Classification of Threat Characteristics. Threat characteristics are classified by artificial means or automated tools; 3) Threat and Security Incident Emergency Treatment. It is involved with precautions, detections, treatment and summaries, etc. of security incidents; 4) Threat Intelligence Sharing. It is described and shared by standardized architecture.

STIX provides the unified architecture to describe security threat intelligence. The core of this architecture refers to 8 threat factors [14] as follows. 1) Observable. 2) Indicators. 3) Incident. 4) Tactics, Techniques, and Procedures (TTP). 5) Campaign. 6) Exploit Target. 7) Course of Action. 8) Threat Actor.

Many institutions have taken advantage of STIX to carry out threat intelligence and information sharing. As long as network security incidents take place, causes, procedures and treatment, etc. related to such incidents can be noted down by STIX to comprehend complete pictures of both threats and incidents.

4. TAXII

As a supplement to STIX in terms of transmission, TAXII (Trusted Automated eXchange of Indicator Information) mainly defines protocol, service and information format, etc. of cyber threat intelligence sharing[15]. At present, cyber threat intelligence is shared by manual, website subscription and automated methods. Not only are sources and subscribers of security intelligence provided by TAXII, but it can be employed by threat management institutions such as government, academic circle and industrial circle, etc. The major threat intelligence sharing modes include Hub and Spoke, Source/Subscriber and Peer to Peer.

According to the objectives of using TAXII service, relevant parties of TAXII are divided into Producers and Consumers. In detail, a producer is a natural person or an organization acting as STI source provider; while, a consumer is the recipient of STI. The producer and the consumer cannot be exclusive to each other and an organization may be either the producer or the consumer of the STI. TAXII service types related to threat information exchange as well as the approaches to acquiring the communication format of services are all clearly described. The relevant types of services are as follows. 1) Push messaging. 2) Pull messaging. 3) Discovery. 4) Query.

Major specifications and files of TAXII are as follows. 1) Service Specification. 2) Message Specification. 3) Protocol Specification. 4) Query Format Specification. 5) Instances of Contents and References. In brief, as standards, STIX primarily plays a role in organizing intelligence, while the key feature of TAXII is about how to transmit intelligence.

5. NIST SP 800-150 Draft

In October 2014, NIST SP 800-150 was issued by the National Institute of Standards and Technology (NIST) and it was the extension of NIST SP 800-61. To be specific, information sharing and coordinated response are extended to the full life cycle (Creation or Collection, Processing, Dissemination, Use, Storage, Disposition) of emergency responses for the cyber security incidents. Such guidance aims at assisting organizations to establish, participate into and maintain the information sharing and collaboration relationships during such a full life cycle. In order to make the organization able to use information sharing and collaboration in a more effective manner in this cycle, the following suggestions are presented in this Guidance [16]. 1) The organization should establish a data resource inventory. 2) The organization should exchange threat intelligence, tools and expertise with sharing partners. 3) The organization should adopt open and standard data formats and transmission protocols to facilitate effective and efficient information exchange. 4) By collecting more data, the organization should analyze and use its incoming data management function to strengthen its own cyber security and capability maturity. 5) The organization should define a self-adaptive network security method used to solve cyber-attacks within the full life cycle. 6) The organization should guarantee that resources required to be shared continuously valid. 7) The organization should maintain a persistent cognition in information security, vulnerabilities and threats to protect sensitive data. 8) The organization should establish necessary infrastructures to guarantee network security.

Furthermore, such a standard also proposed that privacy issues should be considered during information sharing. Sensitivity of information is of vital importance. In addition to following memorandum of understanding, non-disclosure agreement or other protocol framework, it is required to abide by laws and regulations such as PII, SOX, PCI DSS, HIPPA, FISMA and GLBA, etc.. At the same time, not only must information exchanged be identified, but its applicable range should also be agreed on.

6. Instances of Machine Readable Security Threat Intelligence

Simultaneously, contents provided by the security threat intelligence generally contain non-machine readable files that analyze and describe attack incidents in detail and event description files in a machine readable form. The greatest difference between traditional security notifications or warnings and the security threat intelligence lies in that the latter is able to offer machine readable intelligence files. Such machine readable intelligence messages can not only be rapidly used by the supported security platforms such as SOC and SIEM, etc. as well as security devices such as firewall, intrusion detection and antivirus, etc., but be used to monitor relevant network behaviors, mainframe and files, etc.. In a word, based on these messages, APT attacks carried out by other nodes can be efficiently discovered and interrupted, so as to realize the whole network cooperation and quick response in a real sense.

Among attachments of APT1 Report released in 2013 by Mandiant [17], a professional security threat intelligence company that has been purchased by FireEye, not only are malicious code family analysis and SSL certificates contained in the APT attacks incorporated, but they also include FQDN (Fully Qualified Domain Name) information related to the domain name used by APT1, MD5 HASH related to malicious codes and related machine readable IOC files in OpenIOC format. Subsequently, MITRE offers machine readable files in a format of STIX 1.1.1 in line with the Mandiant report.

7. Conclusions

As the threat intelligence service becomes increasingly popular, information security gradually steps into an era of data-driven security. Masses of threat data make the security team overwhelmed; and, the aggregation of these data requires both ideological transformation and threat intelligence maturity so as to achieve a better risk avoidance effect. Otherwise, data collection for the purpose of owning them not only has no benefits, but has the capability to weaken the power of security intelligence planning practically. After all, threat intelligence has become a problem of big data. At the same time, threat intelligence may be also internal threats from the “Enemy Within” that covers employees with operating miss as well as equipment or devices out of a problem. Therefore, it is necessary for enterprises to carry out internal inspecting to define their internal and external vulnerabilities, together with internal risk assessment and formulation action plans.

The day we adopt a single technique or service to solve all emerging challenges has gone forever. It is likely for enterprises to break the circle of passive response, and tactical and technology-leading investment so as to utilize the existing security budget more effectively by thoroughly understanding the mode of thinking, the action route and the target selection criteria of attackers. For an enterprise, the most important thing is the truly critical perspectives of itself environment. Threat intelligence sharing can help identify the known risks. Moreover, by self-training associated with knowledge available and possessing threat intelligence programs particularly customized according to itself environment, threat intelligence sharing is also beneficial for the enterprise to prevent cyber-attacks. In addition, by virtue of threat intelligence, on one hand, the enterprise sets up correct security management objectives. On the other hand, both the enterprise and the security service provider attach more importance to specific values of the enterprise itself, so as to further focus on enterprise security risks and security constructions from a view point of value features together with the driving force of enterprise security compliance. Hopefully, more investments in security constructions are positive and effective, and assistances can be provided to enterprises to defend their most valuable assets and information in a more valid manner.

8. Acknowledgment

This work was supported by the Natural Science Foundation of Shanghai (15ZR1418500), and the Project of Shanghai Science and Technology Committee (15110500700).

9. References

[1] http://www.secdoctor.com/html/xueshu/33791.html.

[2] Jun Fan, *Secret cyber threat intelligence*. Information Security and Communications Privacy, 2015, 12: 76-77.

[3] Definition: Threat Intelligence. https://www.gartner.com/doc/2487216/definition-threat-intelligence.

[4] iSIGHT Partners. https://www.isightpartners.com/.

[5] SANS Information Security Research. http://www.sans.org/.

[6] http://www.sec-un.org/threat-intelligence-is-what.html.

[7] http://x-cti.org/.

[8] https://www.sec-un.com/.

[9] [Yang Zeming, Li Qiang, Liu Junrong, etc. *Research of Threat Intelligence Sharing and Using for Cyber Attack Attribution*. Journal of Information Security Research, 2015, Vol.1(1):31-36.

[10] Wan Tao, *Establishment of China's New Network Security Concept is imperative*. China Information Security, 2015, No.11: 47-53.

[11] http://www.sec-un.org/nuke-classmates-shared-security-threat-intelligence~/.

[12] http://www.sec-un.org/nuke-students-foreign-open-source-threat-intelligence~/.

[13] Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression. http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.0.pdf.

[14] http://www.sec-un.org/information-on-perceptions-of-information-security-threat-intelligence~/.

[15] http://www.sec-un.org/threat-information-structured-machine-readable-taxii-standard-sharing/.

[16] http://www.sec-un.org/united-states-cyber-threat-intelligence-sharing-guidelines-draft-nist-sp-800-150-draft/.

[17] http://www.sec-un.org/mandiant-security-threat-intelligence-instance-apt1/.