International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 14, Number 5 (2021), pp. 396-399

Strategic AI-driven Intelligence Modelling for Identification and Mitigation of Cyberattack on Banking Systems

Amina Baba Adam[1], Ashu Abdul[2]
[1]*Department of Electronics and Communication Engineering, SRM University AP, India.*
[2]*Department of Computer Science and Engineering, SRM University AP, India.*

Abstract
Cyber-criminal groups are known for their innovative multi-staged attacks. Their attacks are focused on the core banking systems, the trading platforms and the ATMs. This paper outlines the applications of artificial intelligence to model a strategic intelligence framework for the identification and mitigation of these attacks deployed in the area of cybersecurity. The intelligence system integrates data collected from the underground community tracking, the unethical hacking databases and a relationship detection engine for adaptation to human intelligence sources. For data intelligence sources, it integrates the compromised data searches, the extraction engines, the phishing kit extraction and the internet fingerprinting. The objective is to assemble a comprehensive strategic threat intelligence system that provides answers to the ever-evolving cyber-attacks targeted at the banking systems. The threat intelligence model strategically adapts relevant data to estimate the risks, prioritize the threats and prepare for the new threats, providing critical information that is tailored, analytical and verified to the organization.

Keywords: Artificial intelligence, banking systems, cybersecurity, threat intelligence

I. Introduction

A cyber or digital threat is defined as any action carried out by an agent to harm, compromise or mislead a target [1]. The agent alone can carry out this action, or it's tactics, techniques, and procedures (TTPs) based on certain known weaknesses of the target. Threat intelligence, on the other hand, is information obtained on the existing or emerging threats to the assets of a target entity based on evidence, including context, indicators, implications and mechanisms of the malicious adversary [2]. This intelligence provides knowledge to understand and make informed decisions on how to mitigate the said threat. Automated threat intelligence (TI) is action-oriented and timely. In the last 10 years, the competence and motive of digital risks in banking sectors have undergone dramatic changes, from micro-scale breaches to major attempts to fully compromise the organization's system of payment and network [3]. Whiles previous threats took advantage of weak target defenses and its existing vulnerabilities, today, hacking resources are easily sourced and attackers providing these services have become organized mercenary groups that develop their exploitation tools [3]. Hence the need for cyber threat intelligence solutions to adopt strategic, and advance detection response models, to meet the cybersecurity needs of today.
Currently, there are 4 types of threat intelligence modelling; strategic, tactical, operational, and technical TI [4]. These are classified based on initial intelligence requirements, data sources, and how the target audience/organization will deploy the information provided by the threat intelligence analyst. This paper puts together a comprehensive threat intelligence model driven by artificial intelligence and machine learning applications to provide strategic solutions for the emerging cyber threats in banking systems [5]. With the emphasis on central and commercial banking systems in Asian and West African countries where study shows, cybercrime groups find more vulnerabilities to exploit in these regions. This situation becomes even direr during the Covid19 pandemic resurgence.

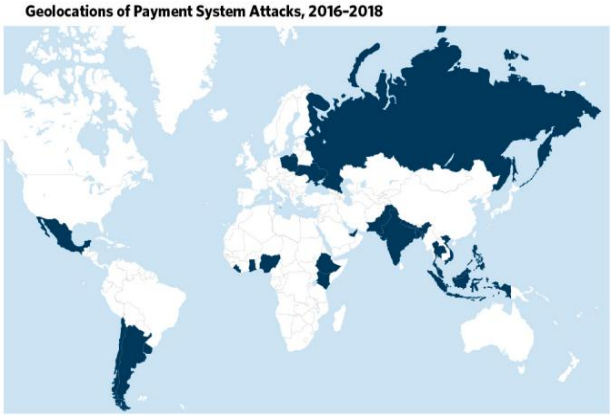

Figure 1. Geographic information showing countries where Payment System attacks are predominant, 2016- 2018 [3]

Figure 2. Working cycle for a threat intelligence framework

II. Overview of Strategic Threat Intelligence

Throughout this paper, strategic intelligence is abbreviated as STI. An STI module lays down a general review of the cyber

threat topology in an establishment to advise high-level policies made by executives and key decision-makers [1][7] [8-9]. This information is used to direct cybersecurity investments. The following are features of a good STI model.

- Tailored with specifications to the security needs of the target organization.
- Analytically adapt data sources relevant to that sector.
- Verified, i.e., tested and demonstrated to operate as required.

II.I Types of targeted attacks

Examining the evolution of banking and payment system cyber-attacks, the current attacks are classified as sophisticated targeted cyber-attacks staged with the intent of financial gain. In recent years, cybercriminal groups have grown smarter to scale up their activities and avoid threat detection with the use of multi-staged threats ranging from Denial of Service (DoS) attacks to

- www attacks
- Structured Query Language (SQL) Injections
- Stealth scanning techniques
- Coordinated distributed denial of service (DDoS) attacks
- Botnets attacks
- Mobile malware attacks [8]

Critical Banking assets at risk of cyber-attacks:

- Customer account records and payment card details
- Retail banking and Point of Sale (POS) platforms.
- Bank to customer communication medium such as the e-mailing system.
- Third-party vendor operations
- Customer Confidence in the banking brand

Attackers exploit the following vulnerabilities:

- Insecure Code and Applications
- Toxic Combinations/Over Entitlements
- Client-Side Software Vulnerabilities
- Unauthorized Privileged User Access
- Unencrypted Data
- Improper Configuration Management
- Network and Operating System Software Vulnerabilities [8]

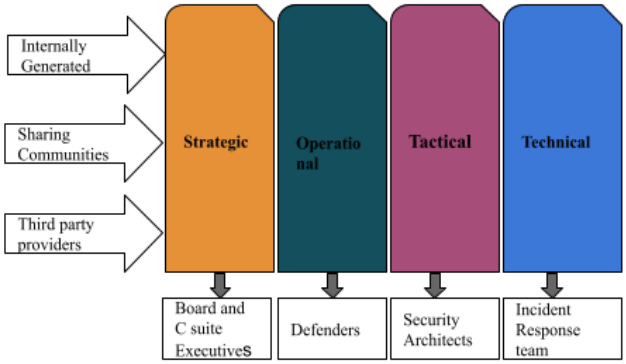

Figure 3. Categories of TI and how they are applied [4]

III. Framework of Strategic Threat Intelligence model

The strategic intelligence framework uses a 2-tier intelligence processing architecture shown in Fig. 4 [7].

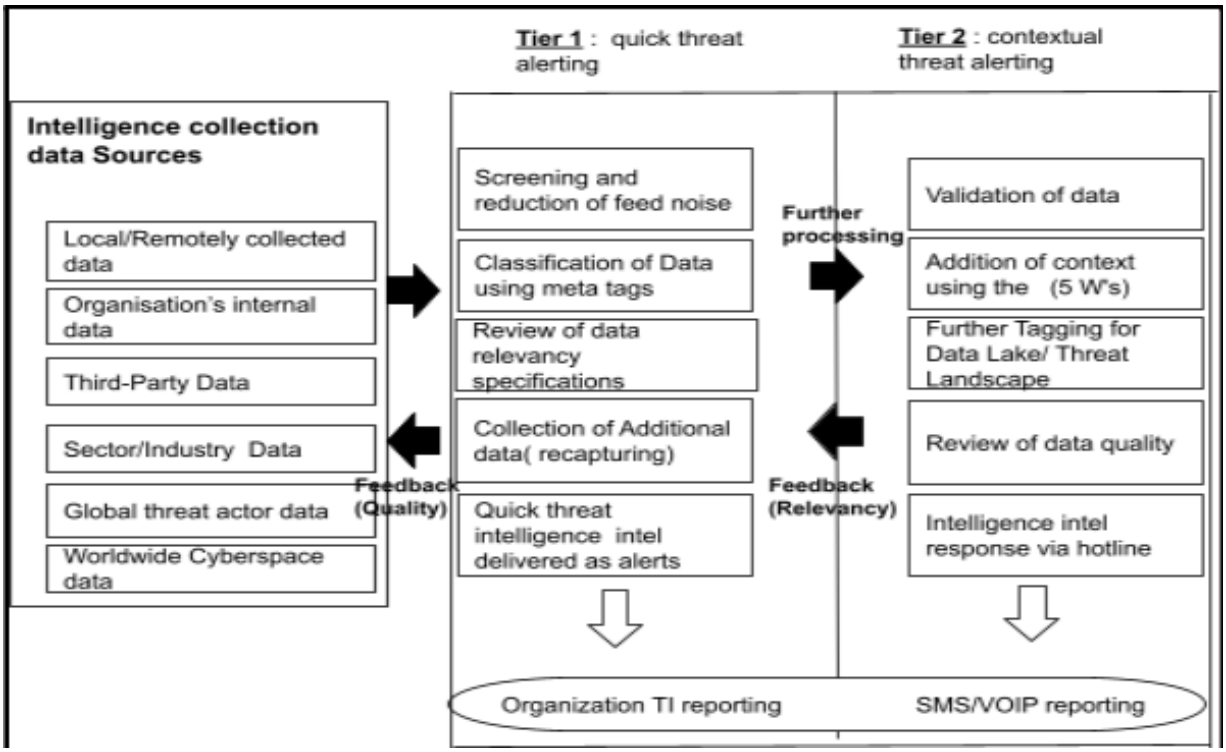

Figure 4. The architecture of the 2-tier intelligence Processing core

The intelligence process answers the why, what, when, where and how(5Ws) of TI to establish the best approaches that can utilize the TI capabilities [9][13] The critical phases of a threat intelligence cycle shown in Fig. 2 is implemented in the framework using Natural Language Processing (NLP) and Machine Learning techniques to drive the automation of the intelligence process.

III.I Direction and Planning

This is the first phase where significant interactions are established between the team of TI analysts and the customer to determine intelligence requirements and priority requirements to most efficiently serve the needs of the customer. From the specified requirements, data and information sources required for the threat intelligence process will be collected. The output at the end of this phase is usually embedded in an intelligence collection plan (ICP). An important guide in this phase is understanding the objectives of the consumer who will utilize the finished product [2] Is the product going to be used by specialized security analysts who require a quick review on a new threat action, or by a board of directors who need a comprehensive understanding of emerging cyber-attack trends to guide investment decisions related to cybersecurity? This latter objective is what is considered for the framework of a strategic threat intelligence program.

III.II Collection

Banking systems generally acquire raw data from a wide range of sources for the collection phase. Data from: the finance industry, third-party vendors, phishing sites and sources, remote points of the organization's internal network, the global cyberspace and attack forums. The important factor at this stage is understanding the assets of the organization that are at risk of a cyber-attack to determine which data sources are relevant for collection into the intelligence process. The collected data is fed into both tier 1 and tier 2 shown in the framework in Figure 4 usually as files containing the indicators of compromise (IoCs), such as hostile IP addresses and domains, file hashes, and network vulnerabilities such as detectable personal details of customers, raw codes and materials from internet websites, published reports or interactive online platforms.

III.III Analysis

Immediately after all the relevant raw data has been gathered, sorting and organization using metadata tags (data tagging) are done to clean and refine the data sets, sieving out unessential details. Natural Language Processing (NLP) and machine learning techniques are used in this phase to analyze materials from a myriad of unorganized data sources over various programming languages to categorize them using ontologies and actions, independent of language to equip analysts to execute more robust and intelligent searches beyond simple key phrases and tags using rules of correlation. The feedback loop enables the threat intelligence process to become dynamic rather than static by using feedback from analysts and other stakeholders to add context and re-evaluate the ingested data sourced both internally and externally. This improves the categorization along with the scoring of techniques used in the intelligence framework. In Tier 1 the feedback loop re-evaluates the characteristic value of the ingested information in terms of quality, i.e., the features within the datasets that make it suitable for the intelligence process. The feedback loop in Tier 2, however, re-evaluates data based on relevancy to measure how connected or related the data collection is to the intended intelligence solution

III.IV Dissemination

What methods will be used to distribute and communicate the finished product to the target user? For TI to be practically useful, it has to reach the intended consumer on time. And should be trackable to ensure the continuity of one intelligence cycle to the next. The finished product should be communicated to the target customer in a common language using meaningful and understandable words. The framework in Fig. 4 shows different alerting methods used in tier 1 and tier 2 because of the different response time and feedback analysis in each. Tier 1 is programmed to distribute alerts to the target organization within 1- 3 mins after data collection and hence is a faster distribution method as compared to tier 2 which takes a response time of 10- 30 mins after data collection to notify the target [7]. The end product of the threat intelligence cycle should give a full report on compromised user credentials and corporate data, warning signs of breaches in the corporate network or threat actors targeting corporate organization and clients, detection of new malware, changes in attack methodology and tactics of threat actors and discussion of exploits and vulnerabilities of the banking system are gathered and fed into the intelligent process.

III.V Review

The review phase is constantly incorporated in each of the other phases and drives the working process of each phase in the TI cycle, to ensure easy authentication and sustainability of the framework.

IV. Conclusion

Relevant Studies shows that cyber-attacks in the financial industry is not diminishing. If anything, the opposite is demonstrated in recent cases: more cybercriminal communities are committed to finding advanced schemes to exploit banks and their clients. This raises a challenge to central and commercial banking organizations looking for cyber solutions to find dynamic and effectively automated threat intelligence modules that are strategically adapted to combat these increasing attacks. Though most of these launched attacks have been targeted at establishments situated in Latin America, Asia and Africa, attack groups are continually expanding their abilities. Major banks that are well-protected cannot afford to become complacent in thinking they do not stand the risk of attack as research studies on threat intelligence provide network defense lessons for everyone, to be a step ahead of the next attack.

V. Acknowledgment

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. The author would like to acknowledge Mr. Sam Dabeesingh, a

partner of leading global cybersecurity company, Group IB, based in Singapore, who put her on the research path of interest in cyber threat intelligence solutions.

References

[1] Bank of England. (2016) CBEST Intelligence-Led Testing Understanding Cyber Threat Intelligence Operations.

[2] Zane Pokorny(April 2019). What is Threat Intelligence? Everything you need to know, Record future.

[3] Adrian Nish, Saher Naumaan (March 2019). The Cyber Threat Landscape: Confronting Challenges to the Financial System - Carnegie Endowment for International Peace.

[4] Digital Shadows Analyst Team. (December 2019) Threat Intelligence: A Deep Dive.

[5] Dehghantanha, Ali., Conti, M., & Dargahi, T. (Eds.). (2018). Cyber threat intelligence Book. New York, NY: Springer International Publishing.

[6] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, "Cyber threat intelligence sharing: Survey and research directions, Computers & Security, vol. 87, Nov.2019.

[7] Allan Thomson. (September 2017) How to implement a threat intelligence program successfully. LookingGlass Cyber Solutions.

[8] Ruth Wandhöfer. (May 2015). Cyber Threats to Retail Financial Services and Payments, Citi-FinSAC-Cyber-Seminar.

[9] Threat intelligence report 2019-2020. The research report, Group-IB (2019).

[10] Threat intelligence report 2018-2019. The research report, Group-IB (2018).

[11] Brown, S., Gommers, J., & Serrano, O. (2015, October). From cybersecurity information sharing to threat management. In Proceedings of the 2nd ACM workshop on information sharing and collaborative security (pp. 43-49).

[12] Barnum, S. (2012). Standardizing cyber threat intelligence information with structured threat information expression (Stix). Mitre Corporation, (pp 11, 1-22).

[13] Mavroeidis, V., & Bromander, S. (2017, September). Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In 2017 European Intelligence and Security Informatics Conference (EISIC) (pp. 91-98). IEEE.

[14] J. E. Lerums, L. D. Poe, and J. E. Dietz, "Simulation Modeling Cyber Threats, Risks, and Prevention Costs," in 2018 IEEE International Conference on Electro/Information Technology (EIT), May 2018, pp. 0096–0101, DOI: 10.1109/EIT.2018.8500240.

[15] Qamar, S., Anwar, Z., Rahman, M. A., Al-Shaer, E., & Chu, B. T. (2017). Data-driven analytics for cyber-threat intelligence and information sharing. Computers & Security, pp(67, 35-58).

[16] Liao, X., Yuan, K., Wang, X., Li, Z., Xing, L., & Beyah, R. (2016, October). Acing the IOC game: Toward automatic discovery and analysis of open-source cyber threat intelligence. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 755-766).

[17] C. Parkerson. (April 2020). Rethinking Threat Intelligence with the LEAD Framework.

[18] Samtani Sagar, Chinn Ryan, Chen Hsinchun & Nunamaker Jay. (2017). Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence. Journal of Management Information Systems. (pp. 34. 1023-1053).

[19] Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber-attacks. Computers & Security, 72, 212-233.

[20] Dalziel, H. (2014). How to define and build an effective cyber threat intelligence capability. Syngress.

[21] Qiang, LI., Zeming, Y., Bao Xu, L., Zhang Wei, J., & Jiang, Y. (2016). A framework of cyberattack attribution based on threat intelligence. In Interoperability, Safety and Security in IoT (pp. 92-103). Springer, Cham.