AttacKG: Extract Provenance Graph-level Attack Variants from Cyber Threat Intelligence Reports

Anonymous Author(s)

ABSTRACT

Threat intelligence are widely adopt in both academia and industry. However, the existing, widely used threat intelligence formats are quite crude [6], hard to defent well-organized APT attacks. Thus, in this paper, we proposed a new graph-based threat intelligence framework.

Another problem that needs to be addressed is the extensive collection of threat intelligence. To address this problem, we ...

1 INTRODUCTION

1.1 Background

#1 Cyber attacks are diversifying.

#2 Threat intelligence and threat reports are helpful tools

Provenance graph as a threat representation tool are already widely studied and adopted [7]. With provenance graph, security analyzers are able to encode system execution history into graphs. Thus provenance graph contain rich semantic information. However, there are still a gap between provenance graphs and human understandable information. Poirot [10] try to solve this problem by involve TTPs and kill chain proposed by MITRE [].

#3 Provenance graph are widely-used and recongnized threat representation approach.

1.2 Related Works

#1 Compare with existing automated threat intelligence collection works.

#2 How our work support provenance graph-based threat detection.

1.3 Our work

#1 Extracting incomplete attack graph from single CTI report.

#2 Delineating behavioural and clustering analysis.

#3 Implement applicaitons.

1.4 Contribution

#1 New threat intelligence representation approach.

#2 Automated threat intelligence collection and management system.

#3 Collected a large amount of threat intelligence and done a through analysis by real-word application.

#4 We provided a open attack dataset.

2 RELATED WORK

2.1 Threat Intelligence

Threat intelligence are widely adopt in both academia and industry. [1, 9]

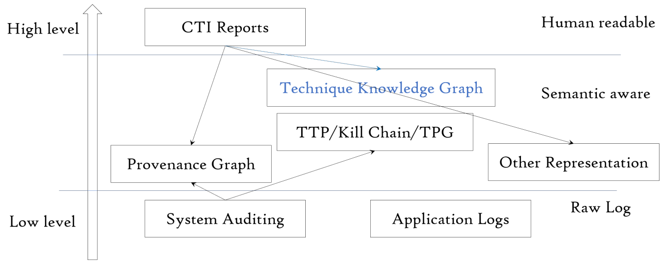

Figure 1: Different Representation of Cyber Attacks.

2.2 Extract threat intelligence from unstructured CTI reports

Existing works try to extract IoC [8], TTPs [4], Attack Chains [12], Attack Graph [2] from unstructed TI. Most recent works tend to extract more detailed and structure information. Ideal CTI should be general to cover more attack cases while detailed to avoid FP. To strike a balance, we need to correlate related attack descriptions and construct a better one.

However, single CTI report cannot provide

2.3 Modeling the cyber threat intelligence (Knowledge graphs for security purpose)

[3, 11] try to model and quantify the underlying relationship among heterogeneous IoCs (Attackers, Device, Platform, Vulnerability, File, Type). These works do not include information about how these IoCs work together (PG), and leave lots of details.

2.4 Threat detection and forensic (Adopt graphs to represent cyber attacks)

[10], etc. can adopt threat intelligence extracted by our system. Accurate and general attack description can ensure detection efficiency and accuracy.

3 BACKGROUND

3.1 Three granularity of variant for PG

#1 Different combination of attack techniques.

#2 Different mplementation of attack techniques.

#3 Different option for attack nodes. [9] [5]

3.2 Problem statement

CTI reports contain rich information needed by detection and analyzer. However, existing reports analysis work focus only on the reports itself, leave out lots of useful information. We propose to adopt TTPs knowledge and Technique/Tactic Knowledge Graph(TKG) to organize the knowledge extracted from reports. And generate more useful attack descriptions.

On the one hand, current CTI sources focus on naïve IoCs, such as bad IPs, malware hashes, etc., without much high-level semantic. Such CTI are neither general nor reliable. [6] On the other hand, unstructed threat whitepapers are vague. – We need new CTI standards.

On the other hand, effective(fast) and efficient(accuracy) detection require accurate attack description. State-of-the-art work rely on manual analysis [10] which is difficult to expand. – We need more and automated CTI.

3.3 Challenges

#C1. How to extract Techniques from Natural-Language CTI? – §??

C1-1. Unstructured Threat Whitepapers Are Vague:

Vague nodes: Lack of explicit node identification; Vague subject:

Vague edges: An operation may corresponds to a series of edges in PG

C1-2. How to find technique dependencies? (Sometimes) S: Employ System Entity/Report/self-defined tags(TCP sockets) as connections

#C2. How to integrate multiple CTI reports? – Contribution 2: Building attack Technique Knowledge Graph. -§??

Observations:

1. A single report most likely covers a fragment of an APT attack?

2.Different reports may conflict due to variant malwares

#C3. How to use the TKG? - What basic function we need to implement on TKG? -§??

4 SYSTEM DESIGN

5 IMPLEMENTATION

6 EVALUATION

Our evaluation aim to answer the following research questions:

#RQ1: How accurate is AKG in extracting threat behaviors from CTI report? – §??

#RQ2: How accurate is AKG in matching (**and finding**) attack variant in different CTI report? – §??

We can adopt MITRE reference to test our technique identification accuracy.

Accuracy + Efficiency *node set matching vs ordered node set matching vs graph(= node set + edge set) matching*

Accuracy *template from MITRE vs template from (MITRE + reports)*

7 DISCUSSION

A TECHNIQUE ATTACK GRAPH EXTRACTED FROM CTI REPORTS

B ATTACK VARIANTS EXTRACTED FROM CTI REPORTS

REFERENCES

[1] Berady, A., Jaume, M., Tong, V. V. T., and Guette, G. From TTP to IoC: Advanced Persistent Graphs for Threat Hunting. *IEEE Transactions on Network and Service Management* (2021).

[2] Gao, P., Shao, F., Liu, X., Xiao, X., Qin, Z., Xu, F., Mittal, P., Kulkarni, S. R., and Song, D. Enabling Efficient Cyber Threat Hunting With Cyber Threat Intelligence.

[3] Gao, Y., LI, X., PENG, H., Fang, B., and Yu, P. HinCTI: A Cyber Threat Intelligence Modeling and Identification System Based on Heterogeneous Information Network. *IEEE Transactions on Knowledge and Data Engineering* (apr 2020), 1–1.

[4] Husari, G., Al-Shaer, E., Ahmed, M., Chu, B., and Niu, X. TTPDrill: Automatic and accurate extraction of threat actions from unstructured text of CTI Sources. In *ACM International Conference Proceeding Series* (2017), vol. Part F1325, pp. 103–115.

[5] Kurogome, Y., Otsuki, Y., Kawakoya, Y., Iwamura, M., Hayashi, S., Mori, T., and Sen, K. Eiger: Automated IOC generation for accurate and interpretable endpoint malware detection. *ACM International Conference Proceeding Series* (2019), 687–701.

[6] Li, G., Dunn, M., Pearce, P., Mccoy, D., Voelker, G. M., Savage, S., and Levchenko, K. Reading the Tea Leaves: A Comparative Analysis of Threat Intelligence. pp. 851–867.

[7] Li, Z., Chen, Q. A., Yang, R., and Chen, Y. Threat Detection and Investigation with System-level Provenance Graphs: A Survey. *Computer & Security 106* (2021), 102282.

[8] Liao, X., Yuan, K., Wang, X., Li, Z., Xing, L., and Beyah, R. 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* (New York, NY, USA, 2016), ACM.

[9] Michael, B., and Rosso, C. YARIX: Scalable YARA-based Malware Intelligence. In *30th {USENIX} Security Symposium ({USENIX} Security 21)* (2021), no. i.

[10] Milajerdi, S. M., Gjomemo, R., Eshete, B., and Venkatakrishnan, V. N. Poirot: Aligning attack behavior with kernel audit records for cyber threat hunting. In *Proceedings of the ACM Conference on Computer and Communications Security* (nov 2019), Association for Computing Machinery, pp. 1795–1812.

[11] Zhao, J., Yan, Q., Liu, X., Li, B., and Zuo, G. Cyber Threat Intelligence Modeling Based on Heterogeneous Graph Convolutional Network. *23rd International Symposium on Research in Attacks, Intrusions and Defenses* (2020), 241–256.

[12] Zhu, Z., and Dumitras, T. ChainSmith: Automatically Learning the Semantics of Malicious Campaigns by Mining Threat Intelligence Reports. In *Proceedings - 3rd IEEE European Symposium on Security and Privacy, EURO S and P 2018* (2018), IEEE, pp. 458–472.