Advances in Computer Science Research, volume 62
2nd Joint International Information Technology, Mechanical and Electronic Engineering Conference (JIMEC 2017)

# Association Analysis Of Cyber-Attack Attribution Based On Threat Intelligence

*Qiang Li [1,2], Zeming Yang [2], Zhengwei Jiang* [2], Baoxu Liu [2], Yuxia Fu [2]*

*1. University of Chinese Academy of Sciences*
*2. Institute of Information Engineering, Chinese Academy of Sciences*
*Beijing, China*
*liqiang7@iie.ac.cn, yangzeming@iie.ac.cn ,jiangzhengwei@iie.ac.cn, liubaoxu@iie.ac.cn, fuyuxia@iie.ac.cn*

**Keywords:** Association Analysis; Threat Intelligence; Cyber-attack Attribution; Constraint Analysis

## Abstract

This paper presented an association analysis method in cyber-attack attribution based on threat intelligence. The method used the local advantage model to analyse the data related to threat intelligence in cyber-attack attribution by combining the intrusion kill chains model and F2T2EA model. Then, this paper introduced and explained association analysis as well as association analysis flow. This flow was composed of four parts: input, association analysis, constraint analysis and output. Then, four types of association analysis were introduced: based on statistic, based on extension, based on behavior pattern and based on probability similarity. Considering about that association analysis is a cyclic iteration process, hierarchical constraint, object constraint, feedback constraint and merged constraint are recommended in detail. Finally, the proposed association analysis method was used in a real emergency response case of targeted attack. The result of case study showed that we can find out much useful information for cyber-attack attribution association analysis based on threat intelligence.

## 1 Introduction

With the rapid development of information technology, a growing number of information infrastructure and data assets connect to the Internet, and more and more businesses rely on the network. Cyber security issues become increasingly serious. Every element of our IT enterprise would be a target, from laptops to network infrastructure. With the widespread deployment of the cyber security devices, conventional cyber-attacks can be effectively prevented and controlled. The key and difficult points of cyber security in research had moved to the prevention and attribution of advanced threat. Advanced threat [1] means the stealthy and high-level intrusion process, among which stand out advance persistent threat and targeted attack. An advanced threat usually targets organizations or nations for business or political motives. The "advanced" process signifies sophisticated techniques which using malware to exploit vulnerabilities in systems. The "threat" process indicates human involvement in orchestrating the attack [2]. Factor in increasing complexity, tightening budgets and a limited pool of security experts, and the prospect for maintaining effective security appears bleak. Defenders must block all attacks; while attackers only need to succeed at one to win. It is hard to defend and trace advanced threat by traditional security protection [3].

One definition of cyber-attack attribution is "determining the identity or location of an attacker or an attacker's intermediary [4]." The target of cyber-attack attribution is finding out the source of attacks among cyber space. According to the recognition of attack media, reconstitution of attack path and the depth and fineness of attribution, cyber-attack attribution can be divided into four levels: 1) The host originating the attack, 2) Intermediary command and control hosts, 3) The individuals carrying out attacks, 4) The political or government organization behind the attacks [5]. Traditional cyber-attack attribution analysis methods include tracing back based on log records, intrusion detection system, malware analysis and honeypots [6], which usually can track and analyse to IP address only. In order to get further information about the attack, we need to make an in-deep analysis on the problems from data sources to analysis methods, especially association analysis.

Traditional association analysis methods in cyber-attack are mainly based on security events. Anderson [7] and Valdes [8] [9] used the manually defined probability similarity and minimal matching rules among intrusion events to build security events association analysis system in project EMERALD. Debar and Wespi [10] proposed a method that utilizing cluster and association in analysis of IDS alerts. This method comprehensively considered similarity and cause-and-effect relationship, and solved the problems partly. Further, researchers proposed using cause-and-effect relationships among attacks to make multistep associations. This method was first presented by Templeton [11] [12]. Then Peng Ning [13] [14] made in-depth and systematic study based on this theory. They came up with a method of cyber security events' association based on preconditions which expressed the alert as a triple, and a technology in association algorithm and building attack scene based on knowledge representation by the triple. Hellerstein [15] at IBM Corporation raised a method that using knowledge base of expert system in association analysis. This method had been used in event association analysis system Tivoli. The methods mentioned above are mainly based on single IDS-mostly security events data in association analysis. Several

analysis processes are complex. Mostly, it is hard to analyse the whole series of event for limit single data.

Another kind of association analysis methods is based on comprehensive information. Morin [16] put forward an IDS alerts associated data model M2D2 which formally described system features, vulnerability information, security tools and alarm events. The model correlated with the information from different source to organize the attack process. F Cheng [17] addressed a multi-core architecture to deal with the challenge in organizing, assessing and processing different types of event information. He designed next-generation SIEM (Security Information and Envents Management) platform based on latest emerged In-Memory data management technique and tested the possible event cluster and association by K-means algorithm. Kotenko [18] proposed an approach by integrating the events in SIEM to describe the whole process of association analysis. Caltagirone [19] proposed diamond model which breaks each cyber event into four vertices or nodes, the event is composed of four core features: adversary, infrastructure, capability and victim. The model provides opportunities to integrate intelligence in real-time for network defense, automating correlation across events, classifying events with confidence into adversary campaigns, and forecasting adversary operations while planning and gaming mitigation strategies. SANS Institute [20] [21] used OODA Loop to rapidly assimilate observations and information. The concept of ODDA Loop was to synthesize those ideas through a process refined over time, select a course of action from among available options and then implement it. By observing the results of the action, new information presents itself, and the loop begins again. The above analysis methods used comprehensive information from deployed systems in association analysis of cyber-attack and designed corresponding analysis framework. But those methods had not in-deep analysis in the effectiveness of result data and the control of association process, especially the identification and choose of data content produced by association analysis, which mainly rely on expert analysis and manual label.

In this paper, we introduced an association analysis method in cyber-attack attribution based on threat intelligence. Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable device, about an existing or emerging menace or hazard to asset that can be used to inform decisions regarding the subject's response to that menace or hazard [22]. The related threat intelligence data was distributed in the whole stages of cyber-attack. By collecting threat intelligence information related to cyber-attack, the proposed comprehensive method built the associations among those data to analyse the whole process of cyber-attack. In detail, this paper designed an association analysis flow. According to the different types of threat intelligence data, four types of association analysis had been considered in the flow, including analysis based on statistic, extension, behavior pattern and probability similarity. What's more, we discussed constraint analysis under the situations of hierarchical constraint, objective constraint, feedback constraint and merged constraint, which were the significant parts of association analysis. Finally, we used a practical case to show the process of association analysis of cyber-attack attribution based on threat intelligence.

The main contribution of this paper is proposing an association analysis method in cyber-attack attribution based on threat intelligence. To our best knowledge, this is the first attempt to discuss association analysis and constraint analysis in cyber-attack attribution based on threat intelligence. We also used the designed association analysis method in practical case study. The result shows that the proposed method is useful in cyber-attack attribution.

The rest of this paper is organized as follows. The next section describes the associated data in cyber-attack attribution. Section 3 discusses the detail process of proposed association analysis method. Section 4 presents a practical case study which using association analysis. Section 5 discusses the result of case study and the limits and shortcomings of analysis method. Section 6 concludes this paper and points out some future research directions.

## 2 Associated data

The associated data can be divided into two kinds: original data and threat intelligence data. According to the experience of emergency response and cyber-attack analysis, the original data mainly consist of three aspects: malware samples, network traffic and log records. The information we can get from malware analysis includes: hash value of samples, behavior characteristics, connected IP address and domain name, etc. From the network traffic data, we can extract IP address, domain name, User-Agent and traffic characters, etc. The log records may cover users' access history, alarm information and operating records, etc.

The context of threat intelligence data can be described by combining two models: intrusion kill chains and F2T2EA model. Intrusion kill chains model was proposed by Lockheed Martin Corporation [23], which defined seven steps of cyber-attack intrusion: reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and action on objectives. Reconnaissance means research, identification and selection of targets. Weaponization refers to coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Delivery points transmission of the weapon to the targeted environment. Exploitation means exploitation triggers intruders' code after the weapon is delivered to victim host. Installation means installation of a remote access trojan or backdoor on the victim system which allows the adversary to maintain persistence inside the environment. Command and Control (C2) points that compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. Actions on Objectives mean that intruders can take actions to achieve their original objectives after progressing through the first six phases. Those kill chains phases can describe the whole systematic process of target and engage an adversary to create desired effects. The F2T2EA model was proposed by United States Air Force and used in intelligence identification, supervision and investigation [24]. The six phases of F2T2EA model are Find, Fix, Track, Target, Engage and Access. During Find step, possible targets are

detected and classified for further prosecution. The Fix step of dynamic targeting includes actions to determine the location of the potential target. During Track step, the target is observed and its activity and movement are monitored. During Target step, the decision is made to engage the target in some manner to create desired effects and the means to do so are selected and coordinated. In Engage step, action is taken against the target. The Assessment phase is common to both deliberate and dynamic targeting of the joint targeting cycle and examines the results of the target engagement [25]. Combining with the two models, we can get a local advantage model based on threat intelligence, which is shown in Figure.1 [26].

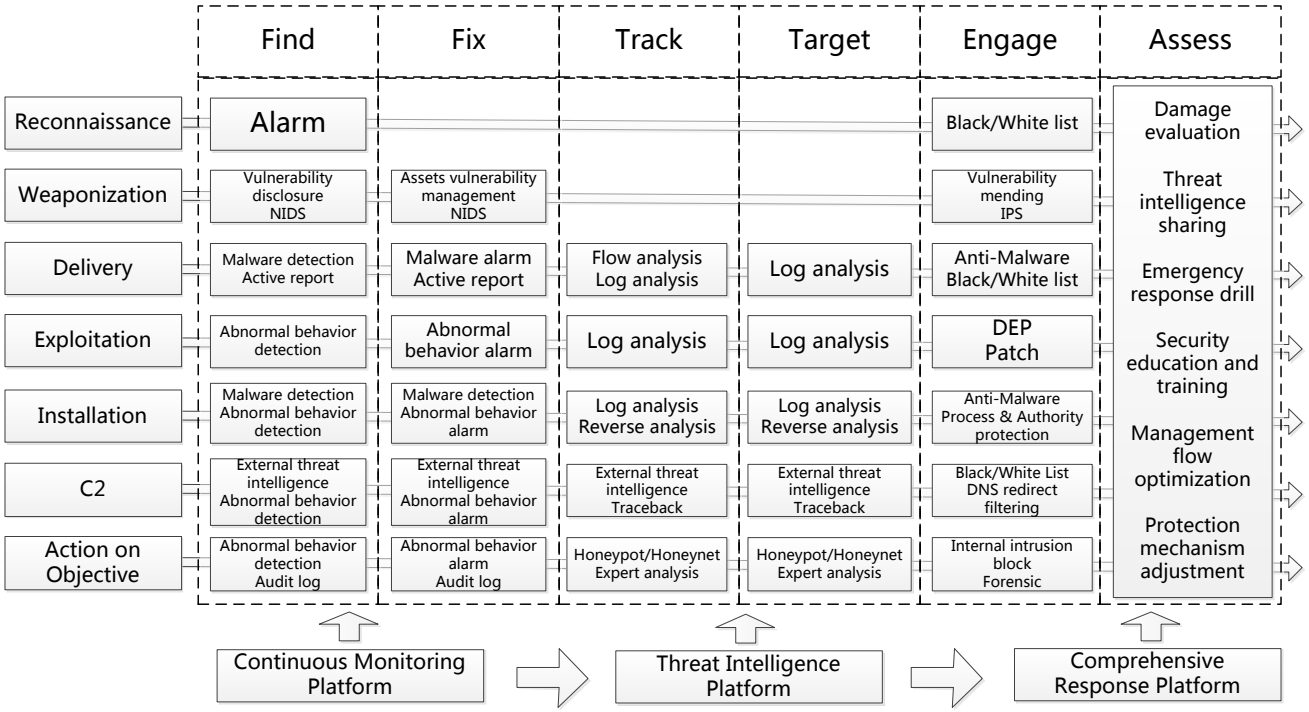


Figure 1 Local Advantage Model Based on Threat Intelligence

The model shows the data we can record and find out during seven steps of intrusion kill chains. The deployed continuous monitoring platform can collect kinds of related information to find and fix cyber-attack. The useful information can be regard as the source of threat intelligence platform. By making full use of threat intelligence information, the output knowledge can be used to track and target the attackers, and also can be seem as the input of comprehensive response platform to engage and assess the security systems and information infrastructure. In Find step of this model, we can get helpful information from suspicious alarm, vulnerability disclosure, NIDS (Network Intrusion Detection System), abnormal behavior detection, malware detection, external threat intelligence and audit log during the seven phases of kill chains. In Fix step, security reinforce scheme refers to assets vulnerability management, NIDS, malware alarm, active report and abnormal behavior alarm, etc. In order to track and target the attackers, we can use flow analysis, log analysis, reverse analysis, trace back, honeypot and expert analysis, etc. In Engage step, responses and solutions include: black and white list, vulnerability mending, IPS (Intrusion Prevention System), anti-malware, DEP (Data Execution Prevention), process and authority protection, DNS redirect filtering, internal intrusion block, and forensic, etc. In final Assess step, assess measures need to be taken, including damage evaluation, threat intelligence sharing, emergency response drill, security education and training, management flow optimization and protection mechanism adjustment, etc.

According to the category and function, the deployed systems include SIEM system, passive DNS system, malware analysis and record system, social engineering information system, etc. SIEM system provides real-time analysis of security alerts which generated by network hardware and application. In cyber-attack association analysis, the input is suspicious IP address, time and alert records, etc. The output is related alerts and records. Passive DNS system owns DNS historical resolution records, including resolved name, resolved data, type, beginning time, end time, count, etc. WHOIS information is also related to the domain name and can provide domain registrant information, including registrant, contact email, registration time and domain status, etc. The input of passive DNS system in association analysis is suspicious IP address or URL, The output is related to DNS resolution records. Malware analysis and record system can analyse malware in static and dynamic, and record the analysis process, results and malware characteristics (e.g. connected IP address or domain, malware signature, extractive features). The input of malware analysis and record system in association analysis is malware samples and malware characteristics, etc. The output is the similar or related malware information. Social engineering information system is composed by the leaked data from various websites

or organizations, like the leaked user information from website CSDN, the documents leaked by Snowden from website WikiLeak, etc. The input of social engineering information system is social engineering information, like email, user name, IP address. The output is the search results, such as similar record and the documents which contain the search record.

## 3 Association Analysis

The association analysis of cyber-attack attribution is based on the associated data mentioned above. The main tasks of this study are association analysis process, types of association analysis and constraint analysis. Details are as follows.

### 3.1 Process

Considering the features of threat intelligence data and the hardship of advanced threat attribution, association analysis is not a linear process, but a cyclic iteration process. The designed association analysis flow is shown as Figure.2.

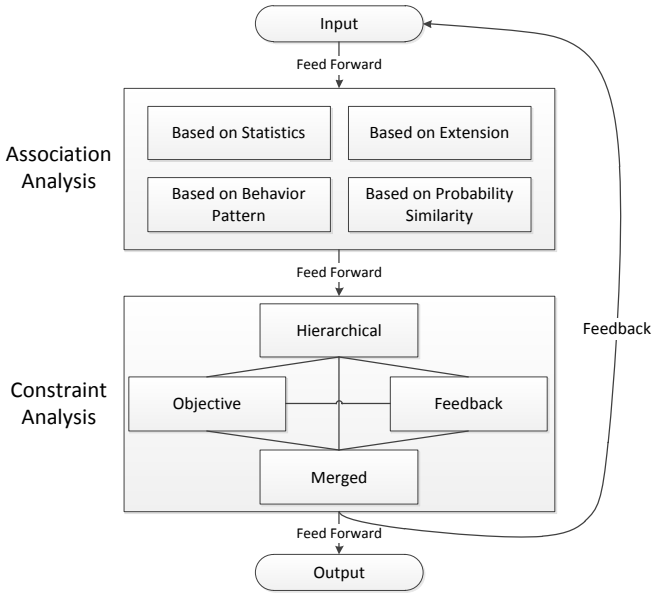


Figure 2 Association Analysis Flow

Association analysis flow shows the process of association analysis of cyber-attack attribution. The whole association analysis constitutes from four parts: Input, Association Analysis, Constraint Analysis and Output.

The Input, which is the start of association analysis, is composed of two parts: original data and feedback data. As the introduction in section 2, the original data mainly consist of three aspects: malware samples, network traffic and log records. Because the association analysis flow is a cyclic iteration process, the feedback data may be the valuable data and further analysis.

The Association Analysis is the course of input data's extension and association. In accordance with the type and content of threat intelligence data, association analysis methods can be classified into association analysis based on statistics, analysis based on extension, analysis based on behavior pattern and analysis based on probability similarity. Detail content will be introduced in the next.

The Constraint Analysis is the process of determining the method of constraint analysis and checking the associated value of data. The results of association analysis can be regard as a graph or a tree. In this case, there are four ways that can be used in constraint analysis. They are hierarchical constraint, objective constraint, feedback constraint and merged constraint. If the analysis results are constrained, the result will be post to the Output. If not, it will feed back to the Input. Detail constraint analysis methods will be discussed as follows.

The Output, which is the results of association analysis based on threat intelligence, also is the end of association analysis flow.

### 3.2 Type of Analysis

Depends on type of threat intelligence data and deployed threat intelligence systems, the association analysis methods are different. We will discuss association analysis methods in conception and content.

**1) Based on Statistics**

Association analysis based on statistics is to find out statistical law and association between clue information and record by analysing the received history records in cyber-attack analysis attribution. The most common of association analysis based on statistics is the log correlation on SIEM platform. Log correlation means uniting the format of all systems' log and analysis of the relation among the clues and records. In the field of cyber-attack attribution, log association analysis means finding out the possible related security events and tracing to identify cyber-attack, especially advanced threat.

The output of this analysis result is the specious log records. It includes content type of events, time, IP address and recording devices. This information can be used to evaluate the attack path, attacking skills and scope of influence.

**2) Based on Extension**

Association analysis based on extension relay on self-building or business threat intelligence systems to find out more detailed and related information. The common extension is expanding the information of IP address and domain by Passive DNS system and WHOIS information. Passive DNS system possess DNS historical resolution records, including resolved name, resolved data, type, beginning time, end time, count, etc. WHOIS information is also related to the domain name and can provide domain registrant information, including registrant, contact email, registration time and domain status, etc. The extended information not only can assess the attack process, but also possibly can ensure the identity of attackers.

**3) Based on Behavior Pattern**

Association analysis based on behavior pattern is to seek out similar and related behavior information from behavior patterns of samples, and then to find out related information based on malware analysis. Normal behavior patterns include

function calls, operant behaviors, key information (e.g. connected IP address or domain, malware signature, extractive features), etc.

The output of this analysis is the recording information of related malware. The associated information can help us analyse the landscape of cyber-attack.

**4) Based on Probability Similarity**

Association analysis based on probability similarity means matching the information extracted from cyber-attack attribution analysis with the data in threat intelligence platform by similarity to find out helpful information. Generally, we used social engineering information system in association analysis based on probability similarity. This system had stored kinds of social engineering information collected from various channels. The information not only includes the username, password, telephone number, email, ID number, but also covers order information, address information, social relationship or even the hotel booking information. Through querying the social information extracted from association analysis of cyber-attack attribution, we can get more detailed and sufficient information about the attackers.

### 3.3 Constraint Analysis

According to the above-mentioned association analysis, the result of association analysis can be regard as a graph or a tree. The original data can be seen as the center node of the graph or the root node of the tree. So the process of association analysis can be considered as a course of graph search or tree search. As shown in Figure.3. Node R means the root node of the tree, Node Np, Ne, Ni point different types of associated information.

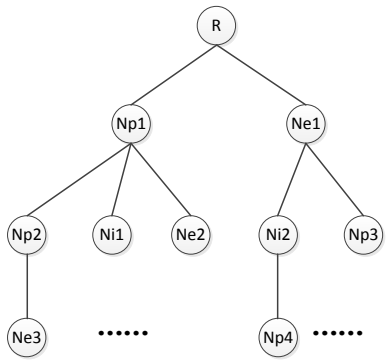


Figure 3 Tree of Association Analysis

If the data in threat intelligence platform is enough, the graph or the tree could be infinite. The purpose of constraint analysis (convergence analysis namely) is to avoid association analysis out of control and get more useful information for cyber-attack attribution at the same time. Convergence analysis is significant in cyber-attack attribution. According to the condition and requirement of cyber-attack attribution, we discussed four kinds of convergence analysis. They are hierarchical constraint, object convergence, feedback convergence and merged convergence. As shown in Figure.4.

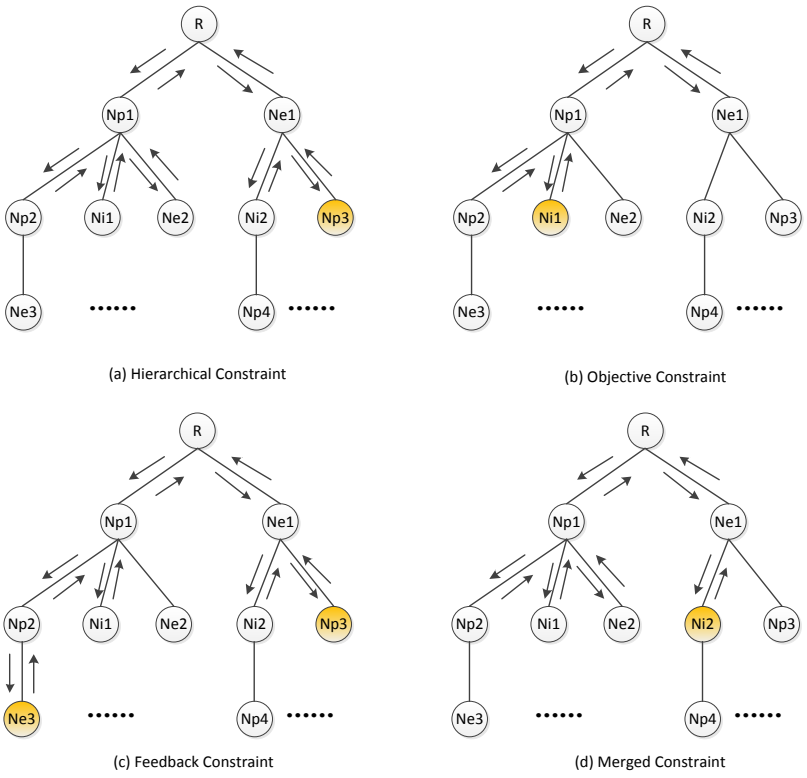


Figure 4 Constraint analysis

**1) Hierarchical Constraint**

Hierarchical constraint means selecting the result of association analysis within certain depth. As shown in Figure.4-a, the depth of tree graph is four and the depth that we selected is three. So the path traversal stops at node Np3. The returned results are the whole traversing node data. The advantage of this method is simple to use, especially used in analysis of normal cyber-attack. The disadvantage is that the quality of result is hard to control. The algorithm is shown as follows:

*Input:* NodeTree: the whole tree graph data
levelNum: the selected depth, must be smaller than the depth of tree
*Output*: QResult: the node data of traversing result
*Variables*: Q: temporary queue

**LabyerTraversebyLevel**(NodeTree, levelNum):

```
initqueue(Q) // Initialize queue Q
initqueue(QResult) // Initialize queue QResult
enqueue(Q,NodeTree.root) //Add to queue
enqueue(QResult,NodeTree.root) //Add to queue
for i from 1 to levelNum:
    node = dequeue(Q) //Output from queue
    for each child of node:
        enqueue(Q,child)
        enqueue(QResult,child)
return QResult //Output the result of hierarchical constraint
```

**2) Objective Constraint**

Objective constraint means searching the expected target until finding out it. As shown in Figure.4-b, our target is the data whose type is Ni. When the first data node of Ni type is found out, data node is returned. The benefit of this method is well-targeted. The shortcoming is low efficiency, especially in analysis of big data. The algorithm is shown as follows:

*Input:* NodeTree: the whole tree graph data
Object: the object of traversal search
*Output*: node: the node data of target
*Variables*: Q: temporary queue

**LabyerTraversebyObject**(NodeTree, Object):

```
initqueue(Q) // Initialize queue Q
enqueue(Q,NodeTree.root) // Add to queue
do:
    node = dequeue(Q)
    if node == Object:
        return node
    for each child of node:
        enqueue(Q,child)
while Q is not empty
```

**3) Feedback Constraint**

Feedback constraint points that adding judging conditions to decide whether it is necessary to continue the association analysis. As shown in Figure.4-c, after judging the data node Ni1, Np3 and Ne3, we stop association analysis and get the traversing node data. The conditions of feedback constraint relay on artificial judgment and previously settings. The advantage of this constraint is the controllable data quality, while the operation is complex.

**4) Merged Constraint**

Merged constraint means that merging the data from association analysis, and adding and finding out the necessary data. As shown in Figure.4-d, our task is to collect more than two node data of Np, Ne and Ni. The association analysis stops at data node Ni2 and returns the traversing node data. Merged constraint is driven by requirements. If these requirements are clear and correct, the effort of merged constraint would be great. The algorithm is shown as follow:

*Input*: NodeTree: the whole tree graph data
MergeList: the list of merged conditions
*Output*: QResult: the node data of traversing result
*Variables*: Q: temporary queue

**LabyerTraversebyMerge**(NodeTree, MergeList):

```
initqueue(Q) // Initialize queue Q
initqueue(QResult) // Initialize queue Q
enqueue(Q,NodeTree.root) // Add to queue
do:
    node = dequeue(Q)
    if MergeList is NULL:
        return QResult
    if node in MergeList:
        MergeList.pop(node)
    enqueue(QResult,node)
    for each child of node:
        enqueue(Q,child)
while Q is not empty
```

## 4 Case Study

We had received an emergency response task from a government office, which had been hacked by spear phishing and water holing. By using proposed association analysis methods above, the analysis process is presented as blew:

1. From the intruded host, we got a malware named “人员与媒体机关发表和接触的新规定.exe”, of which MD5 value is “789b73d80effb4332be17a681ecfaf03”. Then we analyzed this malware with sandbox as well as manual work.

2. Through deep analysis, we found that the operation of malware had gone through four stages: initialization, start, maintenance and remote control. The goal of initialization stage is creating a copy of itself and starting the malware by

right arguments. The task of start stage is detecting the running environment and releasing the function of malware. Maintenance stage is to start remote control function by injecting code. The remote-control stage is achieved by the file of dynamic link library "Bundle.rdb". In these stages, the malware would release three files during runtime, including a copy of itself, QQ.exe (md5: e99c6af520e70b09ade766f13b4e9522) and Bundle.rdb (md5: b77040aff65f5a6934bdcb2abe11abfd). As shown in Figure.5.

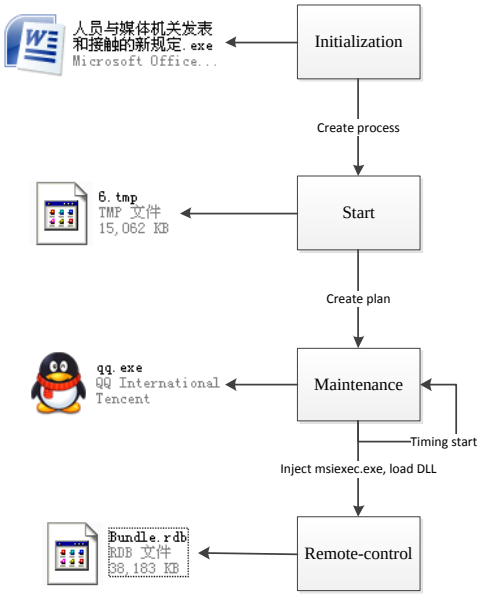


Figure 5 Running stages

3. Based on the network behavior analysis, we found that the malware would visit three domains: sin04s01.listpaz.com, zone.mizove.com, active.soariz.com via one of ports 80, 443, 5430, 5900, 52673.

4. Associating the information with the data in threat intelligence platform, we can get an association graph. As shown in Figure.6.

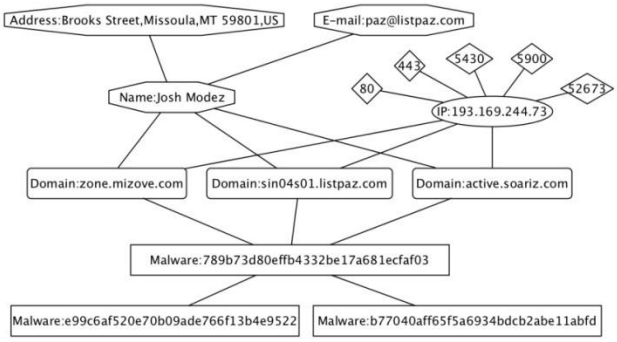


Figure 6 Original Association Graph

5. In accordance with the local behaviors of malware, network behaviors and attacking processes, this malware would be a malware variant of APT OceanLotus (APT-C-ΘΘ) [27] other than the method of code encryption. Combined with the threat intelligence data in the report and threat intelligence platform, we can get a new association graph, as shown in Figure.7.

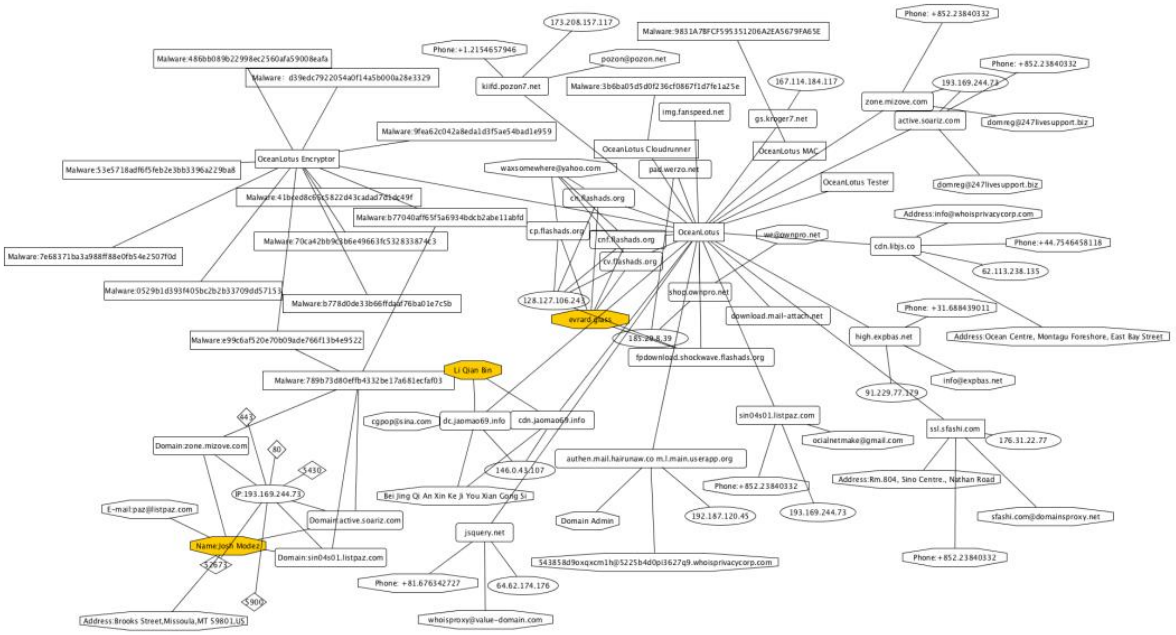


Figure 7 Association Graph extended by OceanLotus

6. We neglected the useless data through objective constraint, feedback constraint and merged constraint to the association analysis, and a new association graph had been made. We can find related information about attackers and attack process. The type of malware in the whole attack process can be divided into OceanLotus Tester, OceanLotus Encryptor, OceanLotus Cloudrunner, OceanLotusMAC. The suspicious attackers are Josh Modez, Li Qian Bin and evrard glass, etc. As show in Figure.8.

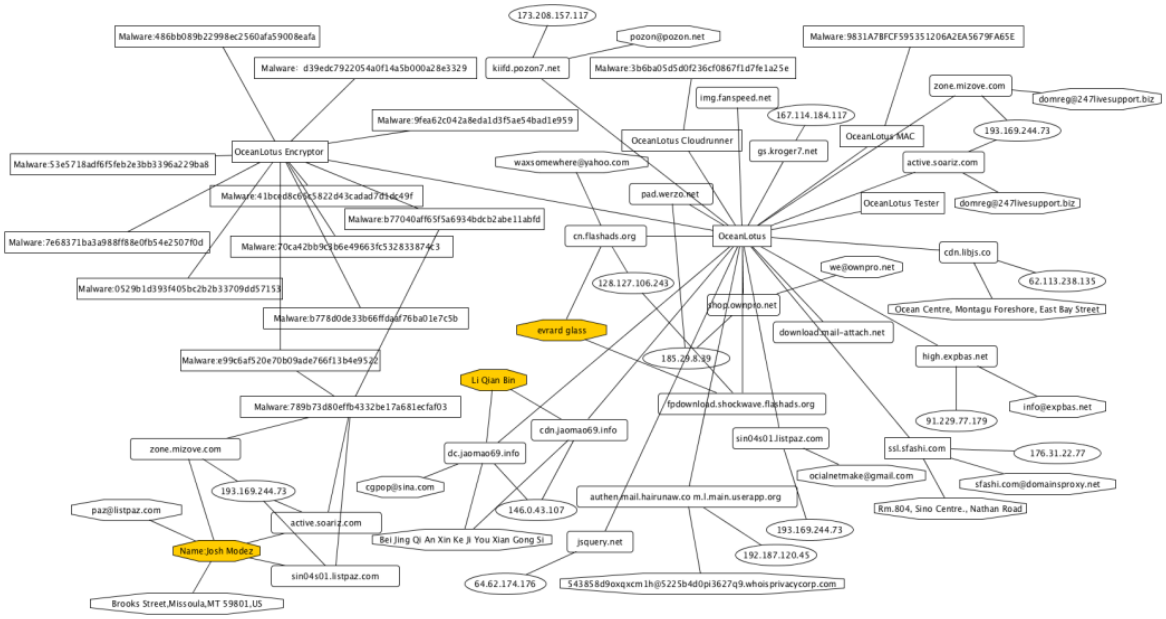


Figure 8 Association Graph after Constraint Analysis

## 5 Discussion

In the association analysis of cyber-attack attribution based on threat intelligence, the main content of association analysis flow includes type of analysis and constraint analysis. Aiming at different types of analysis, this paper discussed four kinds of analysis: based on statistic, based on extension, based on behavior pattern, based on probability similarity. The related technology of this part was comparatively mature, so this paper did not go into the content of association analysis in detail. The main work is to summarize and classify the types of association. In the part of constraint analysis, this paper used simplified tree graph and algorithm to describe and introduce constraint in association analysis.

The case study is a process of analysing cyber-attack, extracting data, expanding data and constraint analysis, the used data include passive DNS records, information related to malware, WHOIS information, etc. The constraint analysis mainly selected and deleted the information unrelated to cyber-attack attribution. In the whole process of case study, the main analysis steps were shown by association graph and auxiliary description about the process of analysis.

## 6 Conclusion and Future Work

In this paper, we came up with an association analysis method in cyber-attack attribution based on threat intelligence. By combining the intrusion kill chains model and F2T2EA model, this method used the local advantage model to analyse the data related to threat intelligence in cyber-attack attribution. Then, this paper introduced association analysis and came up with association analysis flow, and explained the types of association analysis and constraint conditions in detail. Finally, we used the proposed association analysis method in a real emergency response case. The result of case study showed that we can find out much useful information about cyber-attack and attacker by association analysis based on threat intelligence. The output data of association analysis can provide some help in cyber-attack attribution.

The main work of this paper is association analysis process, types of association analysis and constraint analysis. In the future, our task is automated association analysis and constraint analysis. Our target is to reduce artificial workload and ensure the recall and precision [28] at the same time. Moreover, for cyber-attack attribution analysis, it needs further analysis and research, such as reasoning analysis and collaborative analysis.

## References

[1] Wikipedia, Advanced persistent threat, https://en.wikipedia.org/wiki/Advanced_persistent_threat, 2016.

[2] Dr. Sam Musa, Advanced Persistent Threat—APT, https://www.academia.edu/6309905/Advanced_Persistent_Threat_-_APT, 2014.

[3] SANS Institute, Beyond Continuous Monitoring: Threat Modeling for Real-time Response, https://www.sans.org/reading-room/whitepapers/analyst/continuous-monitoring-threat-modeling-real-time-response-35185, 2012.

[4] Wheeler, David A., and Gregory N. Larsen. Techniques for cyber attack attribution. No. IDA-P-3792. INSTITUTE FOR DEFENSE ANALYSES ALEXANDRIA VA, 2003.

[5] Shixiong Zhu, Traceback Cyber Attacks, 2015.

[6] KANTZER, KENNETH HAN-WEI. CYBER ATTACK ATTRIBUTION: AN ASYMMETRICAL RISK TO US NATIONAL SECURITY. Diss. Princeton University Princeton, New Jersey, 2011.

[7] Andersson, Dan, Martin Fong, and Alfonso Valdes. "Heterogeneous sensor correlation: A case study of live traffic analysis." IEEE Information Assurance Workshop. 2002.
[8] Valdes, Alfonso, and Keith Skinner. "Adaptive, model-based monitoring for cyber attack detection." International Workshop on Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, 2000.
[9] Valdes, Alfonso, and Keith Skinner. "Probabilistic alert correlation." International Workshop on Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, 2001.
[10] Debar, Hervé, and Andreas Wespi. "Aggregation and correlation of intrusion-detection alerts." International Workshop on Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, 2001.
[11] Guha B, Mukherjee B. Network security via reverse engineering of TCP code: vulnerability analysis and proposed solutions[J]. IEEE Network, 1997, 11(4): 40-48.
[12] Ko, Calvin, Manfred Ruschitzka, and Karl Levitt. "Execution monitoring of security-critical programs in distributed systems: A specification-based approach." Security and Privacy, 1997. Proceedings., 1997 IEEE Symposium on. IEEE, 1997.
[13] Ning, Peng, Yun Cui, and Douglas S. Reeves. "Analyzing intensive intrusion alerts via correlation." International Workshop on Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, 2002.
[14] Ning, Peng, et al. "Techniques and tools for analyzing intrusion alerts." ACM Transactions on Information and System Security (TISSEC) 7.2 (2004): 274-318.
[15] Hellerstein, Joseph L., Sheng Ma, and C-S. Perng. "Discovering actionable patterns in event data." IBM Systems Journal 41.3 (2002): 475-493.
[16] Morin, Benjamin, et al. "M2D2: A formal data model for IDS alert correlation." International Workshop on Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, 2002.
[17] Cheng, Feng, et al. "Security Event Correlation Supported by Multi-Core Architecture." IT Convergence and Security (ICITCS), 2013 International Conference on. IEEE, 2013.
[18] Kotenko, Igor V., Dmitry S. Levshun, and Andrey A. Chechulin. "Event correlation in the integrated cyber-physical security system." 2016 XIX IEEE International Conference on Soft Computing and Measurements (SCM). IEEE, 2016.
[19] Caltagirone, Sergio, Andrew Pendergast, and Christopher Betz. The diamond model of intrusion analysis. CENTER FOR CYBER INTELLIGENCE ANALYSIS AND THREAT RESEARCH HANOVER MD, 2013.
[20] Hardy, M. G. "Beyond Continuous Monitoring: Threat Modeling for Real-time Response." SANS Institute (2012).
[21] Osinga, Frans PB. Science, strategy and war: The strategic theory of John Boyd. Routledge, 2007.
[22] Gartner, Definition: Threat Intelligence. https://www.gartner.com/doc/2487216/definition-threat-intelligence, 2013.
[23] Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains." Leading Issues in Information Warfare & Security Research 1 (2011): 80.
[24] Tirpak, John A. "Find, Fix, Track, Target, Engage, Assess." Air Force Magazine 83.7 (2000): 24-29.
[25] Joint publication, Joint Targeting, http://www.bits.de/NRANEU/others/jp-doctrine/jp3_60(07).pdf, 2007.
[26] Qiang, Li, et al. "A Reasoning Method of Cyber-Attack Attribution Based on Threat Intelligence." World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering 10.5 (2016): 773-777.
[27] Qihoo 360, APT Ocean Lotus Report, https://ti.360.com/upload/report/file/OceanLotusReport.pdf, 2015.
[28] Schütze, Hinrich. "Introduction to Information Retrieval." Proceedings of the international communication of association for computing machinery conference. 2008.