IEICE TRANS. INF. & SYST., VOL.E101–D, NO.11 NOVEMBER 2018

PAPER Special Section on Information and Communication System Security

Modeling Attack Activity for Integrated Analysis of Threat Information

Daiki ITO[†], **Kenta NOMURA**[†], **Masaki KAMIZONO**[†], ***Nonmembers***, **Yoshiaki SHIRAISHI**[††a)], ***Senior Member***, **Yasuhiro TAKANO**[††], ***Member***, **Masami MOHRI**[†††], ***and*** **Masakatu MORII**[††], ***Senior Members***

SUMMARY Cyber attacks targeting specific victims use multiple intrusion routes and various attack methods. In order to combat such diversified cyber attacks, *Threat Intelligence* is attracting attention. Attack activities, vulnerability information and other threat information are gathered, analyzed and organized in threat intelligence and it enables organizations to understand their risks. Integrated analysis of the threat information is needed to compose the threat intelligence. Threat information can be found in incident reports published by security vendors. However, it is difficult to analyze and compare their reports because they are described in various formats defined by each vendor. Therefore, in this paper, we apply a modeling framework for analyzing and deriving the relevance of the reports from the views of similarity and relation between the models. This paper presents the procedures of modeling incident information described in the reports. Moreover, as case studies, we apply the modeling method to some actual incident reports and compare their models.

key words: *diamond model, threat intelligence, cyber kill chain, incident report*

1. Introduction

Sophisticated and sustained targeted attack is on an increasing trend. The attack is executed through multiple intrusion routes and using various attack methods as one of the countermeasure. There is a system called SIEM (Security Information and Event Management). It manages logs collected from network devices, security devices, and applications in a system and detects intrusion from various routes. It alerts at detecting intrusion. Sometimes, it is difficult to respond to unknown attacks, if the relation of multiple events is analyzed with logs collected by only own organization. For the purpose to counter the various attack, *Threat Intelligence* is attracting attention. Threat Intelligence is knowledge obtained by gathering, analyzing and organizing threat information like attack activities and vulnerability information and it helps organizations to figure out their risks.

By utilizing Threat Intelligence, effective response is possible if an incident has actually occurred, because the next attack activity can be predicted from past cases. For example, combining SIEM with Threat Intelligence enables to clarify how the malware alerted with SIEM was used in the past and the relation with IP addresses or domains not used in the alerted attack. For utilizing threat information and vulnerability information as Threat Intelligence, it is desired that an information complements missing information each other by integral analysis. As one of the example of the threat information, there are incident reports issued by security vendors. For the purpose of calling attention and disseminating information, actual case and trend of incidents are disclosed in the reports, and they contain information of attack methods, intrusion routes, behavior of malware, and targeted victims in the incidents. The vendor dependent reports are different formats, therefore it is difficult to compare each other. However if the reports written with natural language has been modeled like Fig. 1 and it has been possible to treat them abstractly, it may be possible to compare the information of incidents.

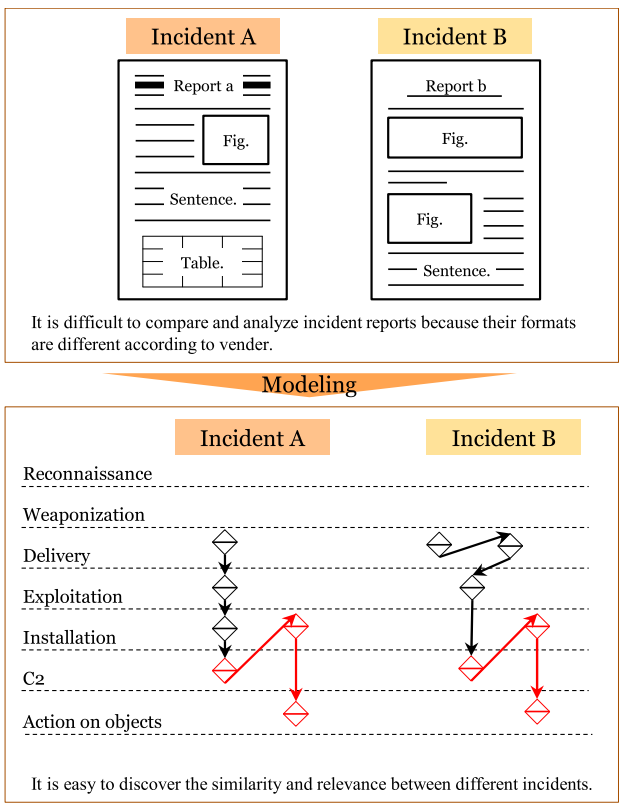

Fig. 1 Discovering the similarity by modeling of reports

Manuscript received November 14, 2017.
Manuscript revised May 13, 2018.
Manuscript publicized August 22, 2018.

[†]The authors are with PwC Cyber Services, Tokyo, 100–0004 Japan.
[††]The authors are with Kobe University, Kobe-shi, 657–8501 Japan.
[†††]The author is with the Gifu University, Gifu-shi, 501–1193 Japan.
a) E-mail: zenmei@port.kobe-u.ac.jp

DOI: 10.1587/transinf.2017ICP0015

In this paper, we give the modeling procedure for the integrated analysis of threat information contained in incident reports. As case study, we compare the incidents published in actual incident reports.

2. Conventional Approaches for Modeling Attack Activities

2.1 Cyber Kill Chain

Cyber Kill Chain has been proposed as the model of intrusion for analysis of attack activities conducted by adversaries using advanced technology and tools or defend effectively from them [1]. This model had been made by expanding Kill Chain, which is the systematic process to obtain the desired effect for the target in military activity. To achieve an attack goal, an adversary needs to develop payload for his intrusion, and his tool like malware needs to intervene inside his target. It moves inside the target network, or executes the action to break confidentially and availability of the target system. Finally, the adversary obtains his desired result. The attack activity is defined as the following seven steps.

1. Reconnaissance: an adversary investigates, identifies and selects a target.
2. Weaponization: the adversary combines malware containing exploit code for remote access with payload which is enable to be delivered, like PDF or Office file.
3. Delivery: the adversary delivers an exploit file made at step2 to a target.
4. Exploitation: when the file is opened, the exploit code is executed, then vulnerable application and system are exploited.
5. Installation: it is possible to access permanently by installing the malware for remote access inside the target system.
6. Command & Control (C2): the adversary can command to inside the target network from external server.
7. Action on objects: the adversary executes the action for final goal so as to collect and destroy data or intrude other targets.

Attack activity for intrusion is executed with step-by-step procedure not only one action. Therefore, defender side can prevent the activity by breaking the chain of phases and appropriate analysis of the activity enables effective defense.

2.2 Diamond Model

Diamond Model is proposed to integrate step-by-step approach of adversary and complement an analysis with Cyber Kill Chain [2]. Attack activity is consisted by a chain of activities. Figure 2 shows an event, which is a minimum unit of the chain. It consists of four elements; *adversary*, *infrastructure*, *capability* and *victim*.

An event is represented like the shape of diamond

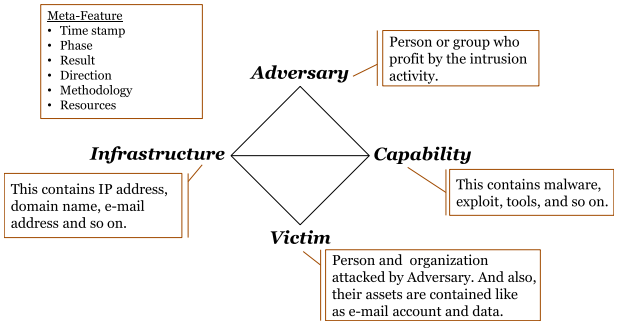

Fig. 2 Diamond Model: an event is defined with 4 elements (adversary, infrastructure, capability, victim) and described as shape of diamond.

which has four apexes. *Adversary*, *infrastructure*, *capability* and *victim* are located at each apex. The four elements are called *core features*. Meta-information like timestamp, phase, result, direction, methodology and resources are called meta-core features. However, we omit the descriptions about meta-core features in this paper. Core features are defined as follows.

Adversary: this describes something which intrudes computer, system, or network to meet some requirements. This is classified into perpetrators executing the attack activity actually and someone or group benefitted from the activity.

Capability: this describes tools or technology used in the event. This contains all technology from manual simple technique to automatic elaborate technology.

Infrastructure: this describes physical or logical communication structure that an adversary delivers capability, maintains control and gains the result from victim. For example, there are IP address, domain name and mail address.

Victim: this is a target which has vulnerability. An adversary uses capability for its vulnerability. This is classified into the target itself like organization and someone or property like a mail account and database which victim has.

2.2.1 Activity Thread

Attack activity can be represented as chain of events which have causal relationship for the purpose of attack. In this paper, an event, causal relationship, and attack activity are represented as a node, a directed edge between nodes, and a directed graph, respectively. Then we define Activity Thread AG and $AG = (V, A)$. V represents a set of events contained in AG and it consists of p subsets. p represents the number of phases. Each event is located at an appropriate phase. A represents a set of edges connecting nodes. In the following, we simply call Activity Thread AG as thread.

It is not always possible to grasp all of events inside a single thread, in some cases, it is necessary to take further investigation or to analyze additional collected data. The analyzing process of identifying shortage information and establishing a new event or edge in a single thread is called

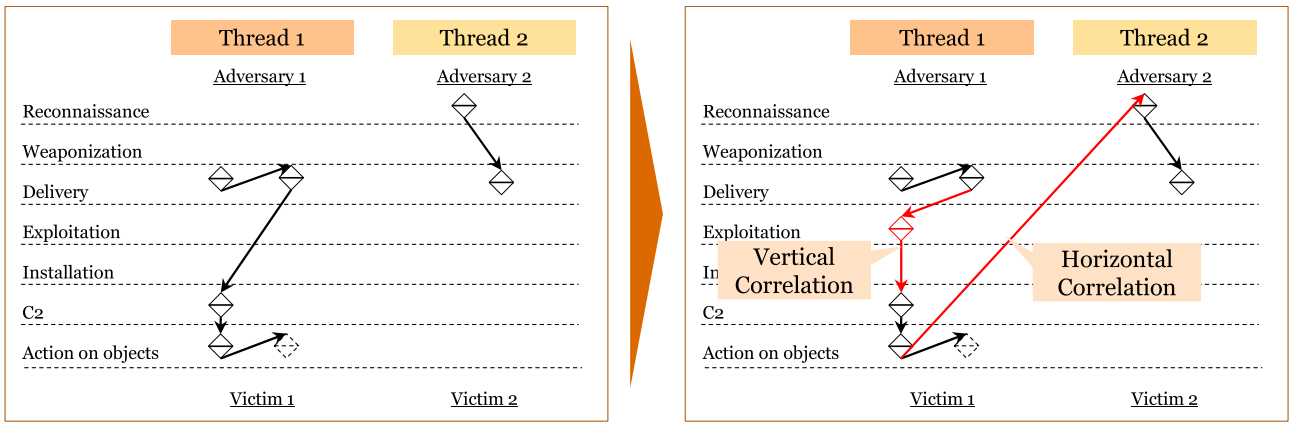

Fig. 3 The examples of Activity Thread represented by a chain of events. It has the two analysis processes: "Vertical Correlation" and "Horizontal Correlation".

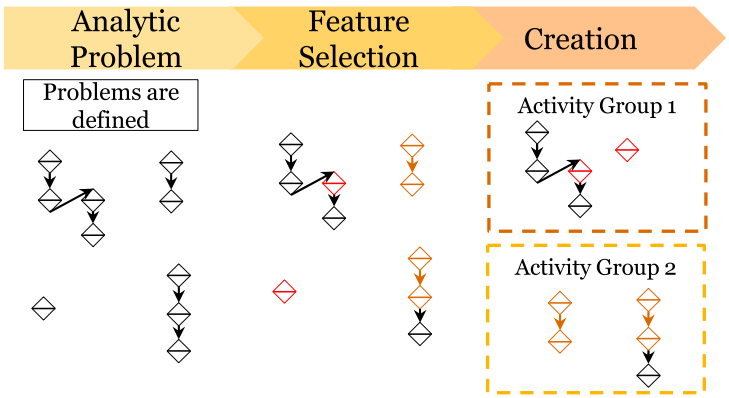

Fig. 4 The example of Activity Groups: threads and events are classified into Activity Group consisted by common features or events by feature vectors.

"Vertical correlation." For example, in Fig. 3, a new event has been added at exploit phase in thread 1 by "Vertical Correlation." To complement other threads, the analyzing process of identifying common shortage information between different threads and associating events according the pair of adversary and victim is called "Horizontal Correlation." For example, in Fig. 3, a new edge has been added between thread 1 and thread 2 by "Horizontal Correlation."

2.2.2 Activity Groups

Events and threads can be grouped based on their similarity of features. For example, in Fig. 4, three activity threads and one event are divided into two groups. The groups are called "Activity Groups," and they are used in analysis to identify common adversary, infrastructure and capability between different threads. This grouping is conducted by the following six steps.

1. Analytic Problem: problems to solve are defined by grouping.
2. Feature Selection: for grouping, core feature and process to be paid attention are selected and defined as feature vectors.
3. Creation: group is made based on the feature vectors extracted from the sets of events and threads.
4. Growth: new event and thread are classified into the group.
5. Analysis: this is conducted to solve the problem defined at Step. 1.
6. Redefinition: group is redefined.

2.3 Challenge for Integrated Analysis

"Vertical Correlation" and "Horizontal Correlation" are analytic process and the goal of them is to fill missing information within a thread or among different threads by additional investigation. However, our goal is to find similar features and relation among different threads by comparing them. Then "Vertical Correlation" and "Horizontal Correlation" do not suit our goal and we do not use them in our proposal.

Configuring "Activity Groups" is an analysis approach which is conducted by a thread unit. The method groups threads and events by feature vectors, as we explained in Sect. 2.2.2. The goal of Activity Groups is to classify multiple events and threads into the group with common features

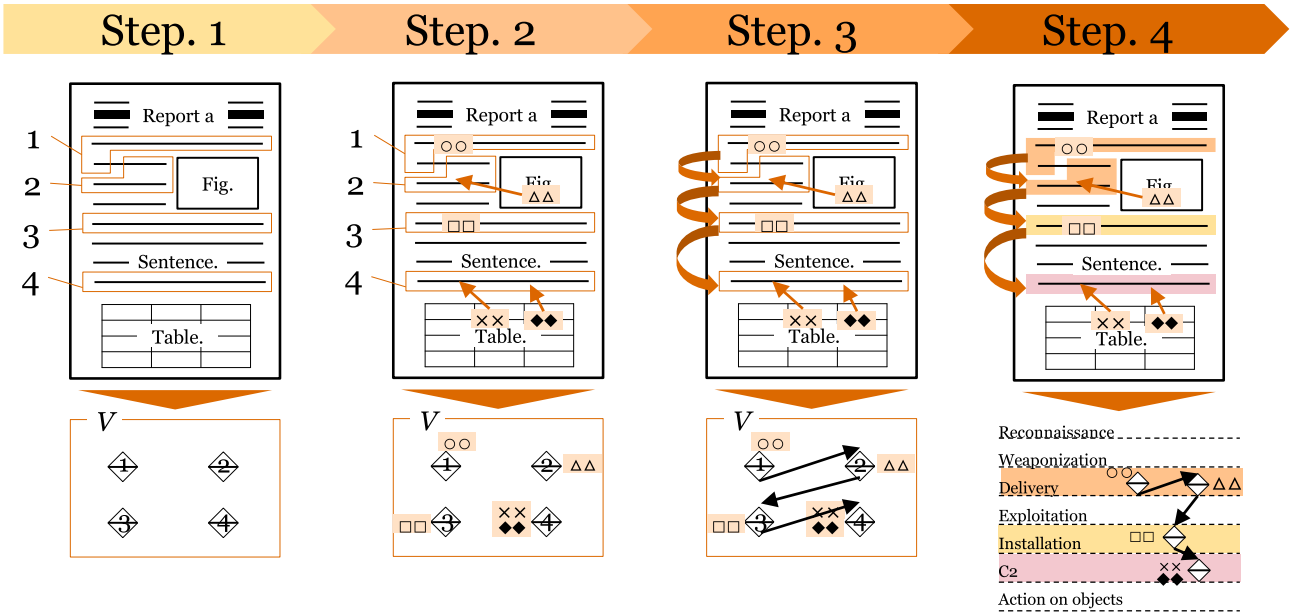

Fig. 5 The flow of modeling threat information from incident reports

and procedures. Its appropriate grouping needs to select appropriate conditions and generate feature vectors. However, it has left challenges to select and generate feature vectors of appropriate Diamond Model for the grouping, and its generalization is difficult because it depends on the environment for implementation.

The challenge towards integrated analysis for threat intelligence is to find the similarity of threat information by discovering common features from threads.

3. Our Approach: Discovering Similarity from Incident Reports

3.1 Discovering Similar Reports by Comparing Threads

In this paper, we represent an incident report, in which attack activity is written, as a thread and confirm whether we can get similar features and procedures by comparing threads. If there is some relevance between threads, it is possible that there is some relevance between incident reports and it is expected that this approach may be help for integrated analysis of threat information for Threat Intelligence.

3.2 Generation Procedure of Activity Thread

Activity Thread is modeled from incident report according to the following procedure and the flow of modeling is described in Fig. 5.

Step. 1 V, which means the set of events, is extracted from an incident report. One event is defined per action. In the report, the action of adversary (e.g. investigation of victim or making a file such as malware), the action of victim (e.g. accessing to malicious URL link or opening a malicious file) and the action of malware (e.g. communication with C2 server or download of additional malware) are contained. The report contains text, figure and table but the description which is enable to be an event is generally written in the text.

Step. 2 Core features are extracted from event. They are discovered from text, figure and table in an incident report. For example, there are address of received mail, vulnerability information used in malware infection, IP address and domain name of C2 server.

Step. 3 A, which means set of edges between events, is calculated. If a second event is happened when one event has been succeeded, these two events are connected by edge. For example, we suppose that malware is installed because a malicious file which is attached to mail has been opened. In this incident, the event that adversary sends email and the event that victim installs the malware by opening the file attached to the email are related each other. Therefore, these two events are connected by edge and then causal relationship is expressed.

Step. 4 The set of events obtained from the above steps is classified into subsets per phase defined in Cyber Kill Chain.

4. Case Study

We confirm whether we can clarify the relevance between threads by using published incident reports. The same adversary uses the same procedure or processes the same intrusion steps. If multiple threads have a common event, the next event which may be happened is enable to be anticipated. Then, we compare the models with paying attention to the structure of threads or connections of events. And also, we compare the models with paying attention to the

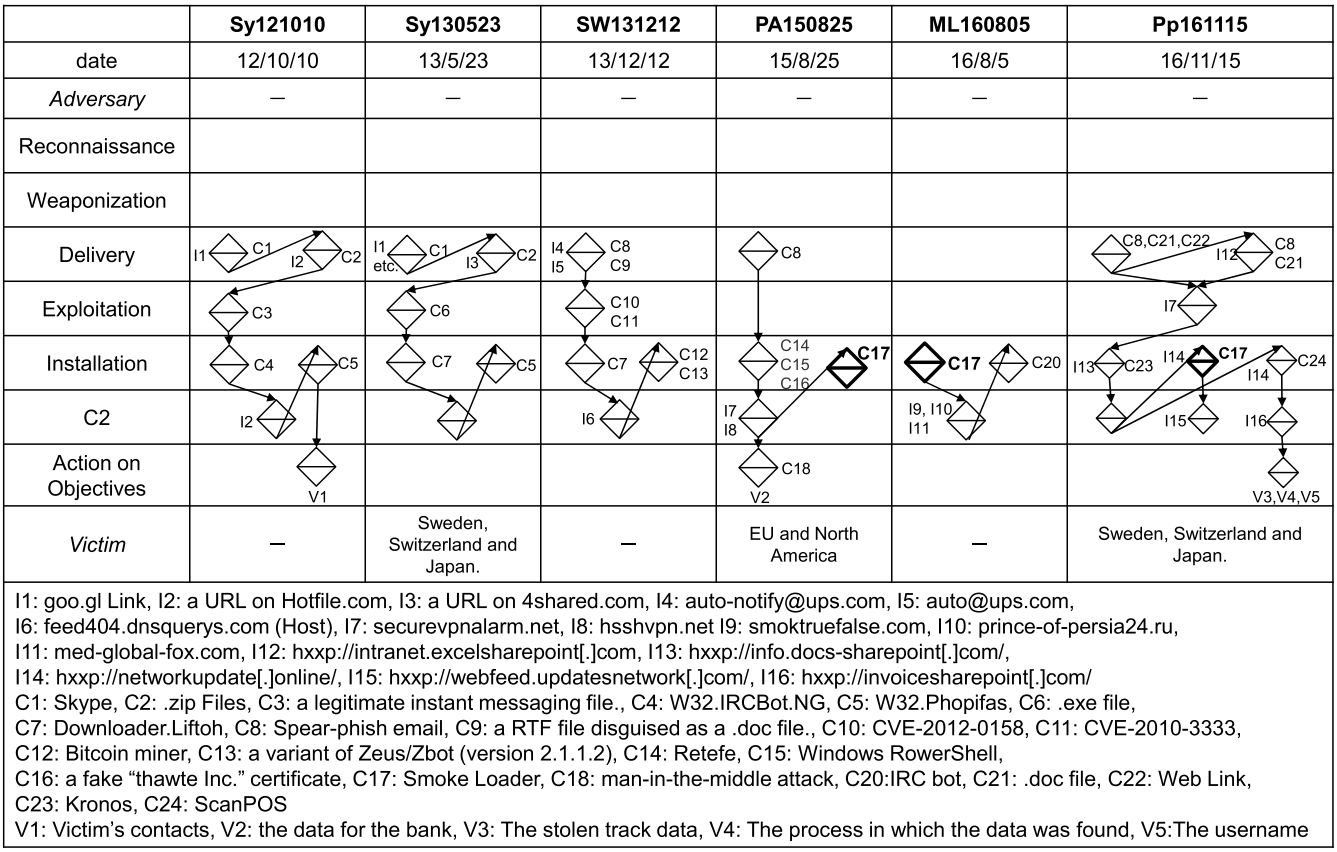

Fig. 6 Discovering the similar report by comparing threads

common events.

4.1 Comparison of Structures of Thread

In this subsection, we compare three threads made from actual incident reports by structure of them.

4.1.1 Contents of Reports

We compare three reports, two of them are published by Symantec [3], [4], one is published at October 10th in 2012 and another is published at May 23th in 2013, and one of them is published by Secure Works [5], it is published at December 12th in 2013. The incident explained in these reports are represented as Sy121010, Sy130523, SW131212, here.

Sy121010 and Sy130523 reports the cases of social engineering attacks for instant message application like as Skype. Message with short URL is sent to users, and when the user opens the link, he is redirected to adversary’s site. Then he is ordered to download a zip file, the file is misrepresented as a proper file and malware is contained in it. If the zip file is executed, the malware intrudes and then other malware is downloaded.

SW131212 reports the case of the attack by spam mail. Malicious RTF file which is misrepresented as “.doc file” is attached to the mail. This RTF file contains exploit for particular vulnerability. If it is succeeded, malware intrudes the victim’s system and then it downloads other malware as secondary payload.

4.1.2 Result of Comparing Threads

The activity threads of Sy121010, Sy130523 and SW131212 are represented in Fig. 6.

Comparing the threads, the structures of Sy121010 and Sy130523 are similar. Both models have the following characteristic points; two events are happened at Delivery phase and Installation event is happened through C2 event. We can find that there are similarities in the way to deliver malware and the action of it. Although the firstly downloaded malware is W32.IRCBot.NG in Sy121010 and it is Downloader.Liftoh in Sy120523, both of them download W32.Phopifas as secondary payload. From the fact, there may be some relation between the adversaries in the two incidents even if the adversaries are not clarified in the reports.

Comparing the threads in Sy130523 and SW131212, the structures after Exploitation phase are similar each other. This is because, in both of the incidents, the same malware is downloaded into victim’s PCs. Although Downloader.Liftoh is malware downloaded at first of each threads, the secondary downloaded malware is different. The malware is delivered by contained in a fake file which is attached to phishing mail in SW131212, and the published

dates of the reports are different. From the facts, it is anticipated that the trends of attacks by adversaries had been changed. Using this modeling method, we can know the trend of cyber attack and behavior of malware.

4.2 Comparison of Common Events of Thread

In this subsection, we compare three threads made from actual incident reports by common events of them.

4.2.1 Contents of Reports

We compare the reports published by Palo Alto Networks on August 25th in 2015 [6], the one published by Malwarebyres LANS on August 5th in 2016 [7] and the one published on 15th November in 2016 [8]. Here, we describe these incidents as PA150825, ML160805 and Pp161115.

PA150825 reports the attack with targeting mail delivering Trojan happened in Western Europe and Japan. A fake file containing the malware called Retefe is attached to the mail which pretends to be a receipt. The malware uses a fake certificate, and finally, an adversary's proxy server executes man-in-the-middle attack. It is reported that Retefe downloads other malware called Smoke Loader. ML160805 is the analysis report of the behavior of Smoke Loader and it reports that the malware downloads other malware through a particular C2 address. Pp161115 reports the attack happened by the malware called Kronos. Kronos also downloads other malwares and one of them is Smoke Loader.

4.2.2 Result of Comparing Threads

In Fig. 6, the activity threads of PA150825, ML160805 and Pp161115 are described. The event contains the malware called Smoke Loader is contained in all of them. The graph structure of PA150825 is different to ML160805 and Pp161115. However it contains a common event, therefore it is anticipated that the subgraph constructed by the events containing Smoke Loader should be complemented to it.

5. Conclusion

For the integrated analysis of threat information, in this paper, we gave the modeling procedure of incident reports which contain the information. As the case studies, we modeled from actual incident reports following the procedure. We compared and analyzed the models, as a result, we found that the relevance between the reports. And also, we analyzed the structure of models and indicated the example that we could complement an attack activity which are not written in the incident reports but may be happened.

Although it is necessary that anyone can generate the same model from the same report for appropriate comparing and analysis, we modeled incident reports manually in this paper. Since automation is essential for efficient investigation, the future work is to design more detailed definition and automatic system to generate the models from incident reports with considering a method of modeling information with different expressions used by vendors (campaign name, detection results, etc.). Validation of applicable scope by increasing number of reports to be verified is also research task.

Acknowledgments

This work was supported by JSPS KAKENHI Grant Number 16K00184.

References

[1] E.M. Hutchins, M.J. Cloppert, and R.M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," Leading Issues in Information Warfare & Security Research, vol.1, pp.80–106, 2011.
[2] S. Caltagirone, P. Andrew, and B. Christopher, "The Diamond Model of Intrusion Analysis," Center forCyber Threat Intelligence and Threat Research, Hanover, MD. 2013.
[3] K. Savage, "W32.Phopifas Cons Over 2.5 MillionClicks with LOL Links," [Online].Available:http://www.symantec.com/connect/blogs/w32phopifas-cons-over-25-million-clicks-lol-links, Oct. 10, 2012.
[4] R. Calvo, "Downloader.Liftoh Cousin to W32.Phopifas?," [Online] Available: https://www.symantec.com/connect/blogs/downloaderliftohcousin-w32phopifas, May 23, 2013.
[5] E. Kumar, "Spam Campaign Delivers LiftohDownloader," [Online]. Available:https://www.secureworks.com/research/spamcampaign-delivers-liftoh-downloader, Dec. 23, 2013.
[6] B. Levene, R. Falcone, J. Grunzweig, B. Lee, and R. Olson, "Retefe Banking Trojan Targets Sweden, Switzerland and Japan," [Online]. Available:http://researchcenter.paloaltonetworks.com/2015/08/retefe-banking-trojan-targets-sweden-switzerlandand-japan/, Aug. 20, 2015.
[7] Malwarebytes Labs, "Smoke Loader – downloader with a smokescreen still alive," [Online]. Available: https://blog.malwarebytes.com/threatanalysis/2016/08/smoke-loader-downloader-with-asmokescreen-still-alive/, Aug. 5, 2016.
[8] Proofpoint Staff, "Kronos Banking Trojan Used to Deliver New Point-of-Sale Malware," [Online].Available: https://www.proofpoint.com/us/threatinsight/post/kronos-banking-trojan-used-to-delivernew-point-of-sale-malware, Nov. 5, 2016.

Daiki Ito received B.E. and M.E. degrees from Kobe University, Japan, 2015 and 2017, respectively. He is currently with PwC Cyber Services LLC, Japan since 2017. His current research interests include cybersecurity and green cloud computing.

Kenta Nomura received B.E. and M.E. degrees from Kobe University, Japan, 2015 and 2017, respectively. He is currently with PwC Cyber Services LLC, Japan since 2017. His current research interests include information security and cryptography.

Masaki Kamizono received his B.E. and M.E. degrees in Computer Engineering from Tokushima University in 2003 and 2005, respectively. He is currently a researcher at PwC Cyber Services LLC, Japan. His research interests include malware dynamic analysis, malware static analysis, and malicious web site detection and analysis technology. He received the Best Paper Award at the 2010, 2011 anti-Malware engineering WorkShop (MWS 2010, 2011). He has also conducted research presentations on security technology at international conferences such as AVAR.

Yoshiaki Shiraishi received B.E. and M.E. degrees from Ehime University, Japan, and Ph.D. degree from the University of Tokushima, Japan, in 1995, 1997, and 2000, respectively. From 2002 to 2006 he was a lecturer at the Department of Informatics, Kindai University, Japan. From 2006 to 2013 he was an associate professor at the Department of Computer Science and Engineering, Nagoya Institute of Technology, Japan. Since 2013, he has been an associate professor at the Department of Electrical and Electronic Engineering, Kobe University, Japan. His current research interests include information security, cryptography, computer network, and knowledge sharing and creation support. He received the SCIS 20th Anniversary Award and the SCIS Paper Award from ISEC group of IEICE in 2003 and 2006, respectively. He received the SIG-ITS Excellent Paper Award from SIG-ITS of IPSJ in 2015. He is a member of IEEE, ACM, and a senior member of IPSJ.

Yasuhiro Takano received the Ph.D. (Info. Sc.) and Dr.Sc. (Tech.) degrees, respectively, from Japan Advanced Institute of Science and Technology (JAIST) and the University of Oulu, Finland, in 2016. He is currently with Kobe University as an assistant professor. His research interests include signal processing for communications engineering.

Masami Mohri received B.E. and M.E. degrees from Ehime University, Japan, in 1993 and 1995 respectively. She received Ph.D. degree in Engineering from the University of Tokushima, Japan in 2002. From 1995 to 1998 she was an assistant professor at the Department of Management and Information Science, Kagawa Junior College, Japan. From 1998 to 2002 she was a research associate of the Department of Information Science and Intelligent Systems, the University of Tokushima, Japan. From 2003 to 2007 she was a lecturer of the same department. From 2007 to 2017, she was an associate professor at the Information and Multimedia Center, Gifu University, Japan. Since 2017, she has been an associate professor at the Department of Electrical, Electronic and Computer Engineering in the same university. Her research interests are in coding theory, information security and cryptography. She is a member of IEEE.

Masakatu Morii received the B.E. degree in electrical engineering and the M.E. degree in electronics engineering from Saga University, Saga, Japan, and the D.E. degree in communication engineering from Osaka University, Osaka, Japan, in 1983, 1985, and 1989, respectively. From 1989 to 1990 he was an Instructor in the Department of Electronics and Information Science, Kyoto Institute of Technology, Japan. From 1990 to 1995 he was an Associate Professor at the Department of Computer Science, Faculty of Engineering, Ehime University, Japan. From 1995 to 2005 he was a Professor at the Department of Intelligent Systems and Information Science, Faculty of Engineering, the University of Tokushima, Japan. Since 2005, he has been a Professor at the Department of Electrical and Electronic Engineering, Faculty of Engineering, Kobe University, Japan. His research interests are in error correcting codes, cryptography, discrete mathematics and computer networks and information security. He is a member of the IEEE.