Vol.2018-IOT-40 No.29
2018/3/6

On Automation and Orchestration of an Initial Computer Security Incident Response

Motoyuki OHMORI[1,a)] Masayuki HIGASHINO[1,b)] Toshiya KAWATO[1,c)] Satoshi FUJIO[1,d)]
Takao Kawamura[1,e)]

Abstract: Computer security has been getting more attentions because a critical computer security incident may cause great damage on an organization such as confidential data breach or malware pandemic. A quick and accurate response against a security incident have been then getting more important. A quick response can reduce not only risk of data breach but also investigating operations. In addition, quickness may enable to contain an incident and prevent malware pandemic. On the other hand, accuracy can avoid unnecessary, excessive and/or wrong operations such as data forensic, re-installing an OS, and isolating an unsuspicious host. In order to realize these quickness and accuracy, this paper discuss to automate and orchestrate an initial incident response against a security incident.

1. Introduction

Computer security has been getting more attentions because a computer security incident may cause great damage on an organization. Since it is difficult to avoid all incidents to happen, a proper and quick response against an incident is important in order to mitigate or minimize damage. The first possible response against an incident is to isolate a *suspicious* host that is observed to behave to compromise security, e.g., communicate with a malicious host such as a Command and Control (C&C) server and The Onion Router (Tor) [1]. This isolation may be initiated as follows. In many cases, a malicious communication is detected by an external organization such as Japan Security Operation Center (JSOC) [2] operated by LAC Co., Ltd, National Institute of Informatics Security Operation Collaboration Services, the so-called NII-SOCS, operated by National Institute of Informatics (NII) [3], government organizations or others. An organization then firstly recognizes a computer security event after receiving an alert of a suspicious communication from an external organization. The organization then makes a triage decision whether the event should be handled as an incident or not. If the event is considered as an incident, the organization then initiates an incident response. An operator in the organization then manually locates and isolates a suspicious host. These location and isolation apparently rely on human operations and operator capability. These location and isolation also load more operations on an operator, and may induce a mistake or longer delay on an incident response. For example, it may require many operations to build a host database, which includes IP address allocation/assignment database, a network topology map and so on. It may be also difficult to maintain and keep the database up-to-date. An operator may make a mistake, e.g., isolating an unsuspicious host. In addition, an operator may forget to share information such as who and when did what operation. This unshared information confuse other operators, e.g., operators other than an operator, who isolates a suspicious host, cannot revert the isolation on a recovery of an incident. On the other hand, a contact person, who is in charge of a management of a suspicious host, may be unable to be immediately contacted due to a business trip or day off. The suspicious host may be then unable to be located, and it may take more than hours to isolate the suspicious host. In order to avoid these mistakes or longer delay, dependencies on human operations must be excluded as much as possible toward the end of the era that relies on human operator's ad-hoc solutions.

To this end, this paper proposes a novel system to automate and orchestrate an incident response. This system requires no host authentication, no IP address allocation/assignment database and no network topology map in advance. This system then automatically receives an alert mail form SOC, isolates a suspicious host, and send a mail to a departmental contact person for further investigations. After an isolation finishes, this system automatically reports its result, i.e., a successful finish or finish with an error, to all operators involved. This system also have an incident tracking function to record all operations. In addition, this system supports a host that frequently moves and its IP address changes. This system also guards against mistakes that wrongly isolates a non-suspicious host or network.

The contributions of this paper can be summarized as follows:

- an operator can manually locate a suspicious host within approximately 3 minutes on average right after an IP address of the host is given,

[1] Tottori University, Koyama-minami, Tottori Japan, 680–8550 Japan
[a)] ohmori@tottori-u.ac.jp
[b)] higashino@tottori-u.ac.jp
[c)] t.kawato@tottori-u.ac.jp
[d)] s-fujio@tottori-u.ac.jp
[e)] kawamura@ike.tottori-u.ac.jp

- the time and a correctness to manually locate and isolate a suspicious host heavily depends upon operator capability,
- the proposed system can locate and isolate a suspicious host within 10 seconds,
- the proposed system can locate and isolate a suspicious host within 1 minutes in an actual environment right after an organization recognizes an event,
- 15 ways are presented to isolate a suspicious host, and it is not enough for a recent malware such as *WannaCry* to just filter out a traffic to/from the Internet.

The rest of this paper is organized as follows. Section 2 defines and clarifies terminologies used in this paper. Section 4 presents automated and orchestrated initial incident response. Section 5 evaluates the proposed system. Section 6 refers to related work. Section 7 finally concludes this paper.

2. Terminology

This section defines terminologies in this paper for clarification as follows.

- SOC: Security Operation Center.
- Event: an observed anomalous behavior. An event can also be an incident.
- Triage: making a decision whether an event should be handled as an incident or not.
- Incident: a special event confirmed to compromise security. An incident may cause a significant disruption of business.
- Incident response: an initial technical countermeasure against an incident. An incident response in this paper refers to initial incident responses until locating and isolate a suspicious host from a network, and further responses are out of scope of this paper.
- Switch: a network switch. A switch in this paper refers to a layer-2 switch only and not a layer-3 switch for simplicity.
- Router: a network router. A router in this paper includes a layer-3 switch.
- Host database: A database comprises an IP address allocation/assignment database, a network topology map, switch port lists, and must be transversely referred by persons involved in an incident.
- IP address allocation: allocating an IP address block to a department or laboratory.
- IP address assignment: choosing an IP address from an allocated IP address block, and assigning the IP address to a host.

3. Motivation

This section states problems in an initial incident response, which motivate authors to automate and orchestrate the response.

3.1 Dependency on Operator Capability

It heavily depends on operator capability to manually locate and isolate a suspicious host. For example, an operator in a organization may manually locate and isolate a suspicious host as follows:

(1) identify a department using an IP address of a suspicious host from an IP address allocation/assignment database,
(2) locate a switch and port accommodating the suspicious host from a network topology map, Address Resolution Protocol (ARP) [4] address table or MAC address table, and
(3) shut down the port or filter out the MAC address.

Regarding (1), an operator who works longer for an organization may memorize an allocation of an IP address block to a department, and the operator can identify the department faster than other operators. Similarly, regarding (2), the operator can locate a switch and port faster than other operators. Regardless of years of continuous employment of an operator, each operator may work in a different place, and an operator may know switches well installed in nearer places but other switches. In other words, each operator has different knowledge about each switch. In addition, some operators may not know how to locate and isolate a suspicious host. Regarding (3), again, some operators may not know how to shut down a port or filter out a MAC address, and how to decide which operation is appropriate.

3.2 Quick Response and Human Operation Delay

A quicker response against an incident is better because a quick response may avoid compromising security and reduce operations. For example, a quick host isolation may avoid compromising confidential information. A quick host isolation also reduces operations to check to see if confidential information is compromised or not. If a suspicious host is not quickly isolated from a network, the host may continue to initiate new communications. In order to make sure that confidential information is not compromised, all communications must be investigated. A quicker host isolation, therefore, can reduce more operations.

A quick host isolation can also avoid a pandemic or epidemic of a malware. For example, *WannaCry* exploits a vulnerability of Server Message Block (SMB) protocol [5], and spreads a malware into other hosts within the same network. In order to avoid secondary infections within the same network, a quick host isolation is necessary.

In addition, a quick response is necessary for a mobile host. A suspicious host may leave a network before the host is located. A quick host locating is necessary.

On the other hand, a manual human operation requires more delay than an automated operation in general. The authors, indeed, have experienced that it took more than 10 minutes to locate and isolate a suspicious host. In order to reduce a delay, an automated operation would be better.

3.3 Building and Maintaining Host Database

Regarding locating a host in a network, it might be considered to build a *host database*. A host database usually comprises an IP address allocation/assignment database, a network topology map and switch port lists. It is, however, difficult to build a host database that persons involved in an incident can transversely refer over an organization. For example, each department builds an own IP address allocation database in the authors' organization, and the database cannot be referred by others. An IP address assignment database may be then built by each laboratory, and cannot be shared among persons involved. In addition, an unified format for these databases is not defined, and its format may de-

pend upon each person who is in charge of managing a database in each laboratory. Under these circumstances, it is difficult for authors to immediately build a host database.

Regarding a host database, it is also difficult to keep the database up-to-date. This is because that it is no incentive for a user to update a database. In authors organization, it is not technically prohibited to assign an IP address that a department or laboratory does not authorize. A user can then intentionally or unintentionally assign an unauthorized IP address to a host, and a host can then communicates. It can be said that a host database may not reflect an actual IP address assignments, and may be useless for a quick response against an incident. In order to solve this issues, ones may be able to technically prohibit a host assigned to an unauthorized IP address from communicating. It may be, however, not feasible because a host authentication must be deployed at all ports at all switches in an organization.

3.4 Human Operation Errors

Nobody makes no mistakes, and an operator sometimes makes a mistake. On a response against an incident, an operator may then make a mistake with higher probability than on a usual operation because the operator is rushed to more quickly respond.

3.5 Inefficiency of Traditional Methods

There are commercial systems to locate and isolate a suspicious host [6]. They, however, employ a traditional method using SNMP and periodically polls a ARP table and MAC address table from a router and switch, respectively. This method is apparently not scalable in terms of the number of network equipment. For example, a polling interval of SNMP is usually 5 minutes. Each polling is done for each switch and router in a network. In authors' environment, there are more than 300 switches. In addition, commercial systems need a large amount of storages citeaxsc, and this may not be scalable. Moreover, authors have experienced that a core router stalls and cannot forward any IP traffic when not so many SNMP packets are received [7]. As described above, traditional methods using SNMP should be avoided.

3.6 Different Authentications for Network Equipment

In authors' environment, there are different models of switches, and these makers also different. In addition, some switches were installed by a maker, and the other switches are installed by a different maker. In this environment, there multiple ways to operate switches such as ssh, telnet, web based GUI and so on. In addition, there are several login accounts, and it is very difficult for an operator to manually and immediately login a switch since it is necessary to consider which vendor installed the switch and what ia an account information.

3.7 Unshared Information among Operators

On an incident response, it is very important to share information among all persons involed in the incident in order to avoid duplicated efforts, meaningless investigations and so on. It is, however, difficult for a person to share information with others because the person may be in hurry to respond to an incident. To make matters worse, a person tends to want to prefer one-to-one communication such as oral communication to one-to-many communications such as mails especially on an incident.

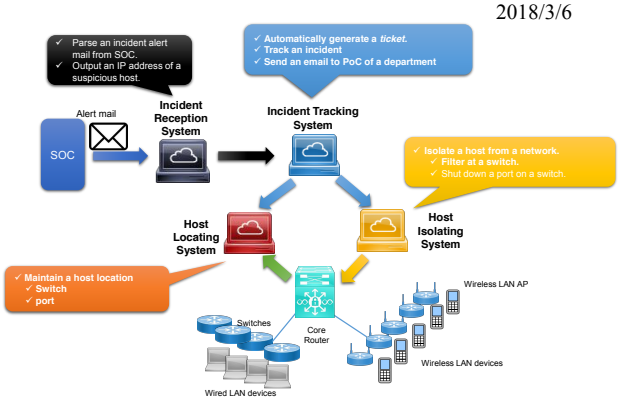

Fig. 1 Incident response orchestration overview.

3.8 Unrecorded Operations

On an incident response, it is often observed that no one knows who did what, how and when, even though a suspicious host is quickly isolated. Since it is possible for an operator to wrongly operate a switch, it is better to record an operation. It is, however, difficult for a human being to memorize or write down what he or she did especially when he or she is in a hurry.

3.9 Vendor Lock-in

Several systems have already supported automation and orchestration of an initial incident response [6]. All switches and routers must be, however, made by the same maker. This incurs vendor lock-in, and this may make it difficult to incrementally replace network equipment year by year.

4. Incident Response Orchestration

This section firstly presents an overview of incident response orchestration and its components. This section then describes each component in much more detail.

4.1 Overview

The incident response orchestration in this paper comprises of four systems: an incident reception system, incident tracking system, host locating system and host isolating system. In **Fig. 1**, all routers and switches employ Link Layer Discovery Protocol (LLDP) [8], or a similar protocol, Cisco Discovery Protocol (CDP), to find neighbors and automatically compute a network topology.

As shown in Fig. 1, the incident response orchestration behaves as follows. An incident reception system receives an alert mail from SOC, parses the mail, and extracts an IP address of a suspicious host. The incident reception system then sends notifies an incident tracking system of the IP address, the alert mail and so on. The incident tracking system then records the alert mail and the IP address. The incident tracking system then resolves the location of a suspicious host, a switch and its port that accommodates the suspicious host, by a host locating system. A host locating system may find a location of a host on demand. Or, the host locating system tracks the host location by polling ARP table and so on. A host host isolating system then isolates the suspicious host from a network.

4.2 Incident Reception System

An incident reception system is in charge of receiving an alert mail from SOC. Unfortunately, some SOCs do not send an alert mail in pre-defined format. It is then unbelievably that some SOCs manually input a message body of an alert mail. Such alert mail then includes inconsistent expressions. For example, an IP address is usually represented in normal dot notation. An IP address, however, sometimes may contains some brackets ([]) before/after dot (.) in order to avoid to unintentionally access to the malicious a host. In order to overcome inconsistent expressions like this, the incident reception system should be able to properly necessary information such as IP address, URL and so on.

4.3 Incident Tracking System

An incident tracking system enables to track responses against an incident by recording each responses. The incident tracking system each incident by a ticket as same as a bug tracking system (BTS). The incident tracking system has an IP address allocation database and Point of Contact (PoC) per address block. Using this database, the incident tracking system then sends an email to PoC when an incident occurs. The incident tracking system is also in charge of bridging other systems.

4.4 Host Locating System

The host locating system locates a suspicious host; the suspicious host is connected to which port on which switch. The host locating system requires only an IP address of the suspicious host, an IP address of a router, time and RD or name of VRF if necessary, and do not requires a pre-defined host database. This nature reduces a load on an operator in an organization to build or periodically update a host database. This nature can then locates even a host that is not registered to such host database.

There are two major methods to locate a host. One is a on-demand method and the other is a proactive method.

4.4.1 On-Demand Host Locating

This method is given an IP address of one of routers and VRF in an organization network, and then locates a suspicious host as follows.

(1) connect to a router, which is given in advance,
(2) look up a route for an IP address of the suspicious host and VRF,
(3) connect to the nexthop router of the route if the route is not *directly connected*,
(4) repeat (2) and (3) until a *directly connected* rout is found, i.e., locate a router that has a *directly connected* route for an IP address of the suspicious host and VRF,
(5) identify a VLAN for the IP address at the router,
(6) locate a *directly connected* router for the IP address on the VRF,
(7) resolve a MAC address of the suspicious host from an Address Resolution Protocol (ARP) [4] table,
(8) identify a port on which the MAC address is seen in a MAC address forwarding table,
(9) discover a neighboring switch on the port,
(10)repeat from (8) to (9) until a neighboring switch is not found,
(11)finally locate a port on a edge switch accommodating the MAC address, and
(12)produces *location information* of the suspicious host.

```
1  def locate_host(core_router, gip, time)
2          # resolve an internal IP address and VRF.
3          (ip, vrf) = resolve_local_ip_address(gip, time)
4
5          # find a directly connected router.
6          router = core_router
7          while router do
8                  route = router.lookup_route(ip, vrf)
9                  if route.is_directly_connected?
10                         break
11                 end
12                 # we cannot control user's or
13                 # departmental router.
14                 if not route.nexthop.is_ours?
15                         ip = route.nexthop.ip_address
16                         break
17                 end
18                 router = route.nexthop
19         end
20
21         vlan = route.vlan
22         mac = router.resolve_mac_address(ip, vlan)
23
24         # locate an edge switch and port.
25         sw = router
26         while sw do
27                 port = sw.mac_address_table(vlan, mac)
28                 neighbor = port.get_neighbor
29                 if neighbor.nil?
30                         break
31                 end
32                 sw = neighbor
33         done
34         return sw, port
35 done
```

Fig. 2 A pseudo code to locate a suspicious host on demand.

One can see more detailed pseudo code in **Fig. 2**. As shown in Fig. 2, note that there is a special case where a departmental router is installed and routes are directed to the departmental router, i.e., an organization-wide administrator cannot operate the departmental router, and a MAC address of the actual suspicious host cannot be resolved. In this case, a MAC address of the departmental router should be resolved and the departmental router should be isolated. This allows an organization to flexibly design an organization network.

4.4.2 Proactive Host Locating

This method collects a location of a host in advance when a host connects and disconnects to/from a network. In order to reduce unnecessary traffic in comparison with traditional methods using SNMP, this method utilizes MAC address authentication and accounting using RADIUS. All ports of all switches that accommodates a edge host is configured to enable MAC address authentication and accounting. It is, however, unnecessary to register any MAC address in a RADIUS server in advance. Instead, a RADIUS server should always authenticate any MAC address.

4.5 Host Isolating System

A host isolating system is in charge of isolating a suspicious host from a network. There are multiple methods to isolate a suspicious host. We have found that methods can be classified from the viewpoint of a type, method, place, supporting a mobile host, containment, collaterally isolating an unsuspicious host and feasibility as shown in **Table 1**. As shown in Table 1, each method has pros and cons. We have then found that there is no method that can be adopted to all cases. For example, an authentication seems to be the best method. It may, however, be difficult to employ an authentication on all ports on all switches because some hosts still do not implement an authentication. A MAC address filtering at an edge switch then seems to be better method. A MAC address filtering cannot, however, be implemented at an edge switch in some cases because some switches cannot simultaneously implement a MAC address and IP or UDP/TCP filtering. These switches, hence, cannot simultaneously implement a MAC address filtering and Web authentication because a Web authentication generally requires UDP/TCP filtering to allow a DHCP communication before an authentication. Web authentication may be required in many cases today, and a MAC address filtering at an edge switch may, therefore, not be feasible.

5. Evaluation

This section evaluates how the proposed automation and orchestration is efficient and effective.

5.1 Host Locating Operation Time

We here measured time of manual and automatic operations of locating a host. We, authors, currently have 5 technical staffs who are in charge of operating our campus network. All technical staffs have been working for our organization for more than 5 years, and memorize a certain degree of the network topology. We then measured the time required for each staff to locate each host under below conditions:

(1) 12 IP addresses are given,
(2) each IP address is on a different network segment, i.e., a different broadcast domain,
(3) some IP address is from a different campus,
(4) 4 different passwords and user name are used for login and privilege accesses to switches and routers for privilege separation,
(5) each technical staff is allowed to obtain information associated with a given IP address from a database such as a department, geographical location, building and so on,
(6) each technical staff should locate a switch and port to which a host given an IP address is connected, and
(7) each technical staff should locate a switch and port only by himself or herself without any advice in advance.

Table 2 then shows the results of the measurements. As shown in Table 2, there were some human operation errors that wrongly located a switch or port. Some operators then required advices to locate a switch, or could not locate a switch or port. It can, therefore, be said that it depends on an operator's skill to locate a host.

Table 2 also shows that a time to locate a host depends on an operator and switch as each standard deviation (SD) of required times is larger. This indicates that an operator may know a switch well but not other switches. Again, it can, therefore, be said that it depends on an operator's skill to locate a host.

In case of the proposed system, each SD for each IP address is small, and each time depends on the number of routers and switches. It can be said that the proposed system can exclude dependencies on a human operation.

Table 2 also shows that a human operator requires 3 minutes on average while the proposed system requires 10 seconds at maximum. It can be said that the proposed system can reduce operation delays.

Table 3 Times to required to isolate a host right after an alert mail is received.

No.	time (sec.)
1	28
2	32
3	47

5.2 Initial Incident Response Time

We here measured time to automatically isolate a host and send a mail to PoC right after an alert mail is received from SOC. **Table 3** then shows the results of the measurements. As shown in Table 3, all initial incident responses were done within 1 min. Before automating an initial incident response, we needed more than 20 min. or even more than several hours.

6. Related Work

NAGAI, Y. et al. investigated and reported differences between ISMSs in national universities in Japan[9]. They also presented their own incident management system using trac[10]. They then reported that their system could record information of only about a half of all security events because some of those events were reported or discussed in meetings and their data was never input to the system.

HASEGAWA, H. et al. proposes the countermeasure support system against incidents caused by targeted attacks [11]. Their system automatically suggests 9 types of traffic filtering to an operator in accordance with a severity of an incident. They, however, consider only a traffic filtering across VLANs at a core router, and do not consider a traffic filtering within a VLAN. Their system then cannot avoid a sort of a malware, e.g., *WannaCry*, to spread within the same VLAN. Their system also assumes that a network configuration is given in advance. In addition, they do not consider a mobile host that moves around in an organization. These are different from our proposal.

ALAXALA Networks Corporation has released AX-Security-Controller (AX-SC) [6] on 2017 that can also isolate a suspicious host. AX-SC, however, employs a traditional method using SNMP to locate a host and periodically polls a MAC address table from a switch. AX-SC, therefore, produces more control traffic and requires more loads on a switch than our proposal. AX-

*1 Less than 10 seconds rounds down to zero second.
*2 A MAC address was not resolved before an advice was given.
*3 A wrong port was located.
*4 A wrong switch was located.
*5 A switch could not be located.

Table 1 Pros and cons of host isolating methods.

Type	Method	Place	Mobile	Containment	Collateral	Feasibility
authentication	authentication	auth. server	good	good	good	poor
physical operation	plug off a cable	edge	poor	good	fair	good
shut down	port	edge	poor	good	fair	good
	VLAN (L2)	edge	poor	good	fair	fair
		router	fair	fair	poor	good
	VLAN (L3)	router	fair	good	fair	good
filter	MAC address	edge (port)	poor	good	good	poor
		edge (FIB)	poor	good	good	fair
		router	good	fair	good	good
	IP address	edge (port)	poor	good	good	fair
		router	fair	fair	good	good
		exit firewall	fair	poor	good	good
	UDP/TCP port	edge (port)	poor	fair	good	fair
		router	fair	fair	good	good
		exit firewall	poor	poor	good	good

Table 2 Times required to locate hosts.

			Traditional manual operations[*1] (min.:sec.)								The proposed system (sec.)		
IP address	routers	switches	A	B	C	D	E	mean	median	SD	mean	median	SD
IP_1	2	4	4:20	3:30	4:00	4:00	14:50	6:08	4:00	4:52	4.311	4.324	0.112
IP_2	1	5	2:30	5:00	8:00	3:00	12:00	5:30	4:00	3:44	8.247	8.312	0.146
IP_3	3	1	2:30	3:30[*2*3]	4:00	0:40	15:10	5:10	3:30	5:44	2.121	2.155	0.095
IP_4	2	2	2:20	4:00	2:50	2:30	8:30	4:02	2:50	2:35	4.420	4.381	0.147
IP_5	3	1	3:30	2:00[*2]	2:20	2:00	3:50[*5]	2:44	2:20	0:52	2.373	2.392	0.090
IP_6	1	2	8:50[*4]	5:00	10:00[*4]	3:30[*4]	18:50[*5]	8:50	8:50	5:12	5.329	5.352	0.160
IP_7	1	3	2:00	4:30	2:00	3:30	11:10	4:38	3:30	3:48	7.047	6.990	0.219
IP_8	2	3	1:40	3:30	2:00	5:00	7:00	3:50	3:00	2:13	3.626	3.645	0.124
IP_9	1	3	13:20	3:30	5:50	3:00	11:10	7:22	5:50	4:39	7.030	7.083	0.252
IP_{10}	2	3	2:50	3:00	2:20	8:00	8:20	4:54	3:00	3:00	3.583	3.591	0.097
IP_{11}	1	3	2:50	2:30	1:50	3:00	16:00	5:14	2:50	6:02	6.915	6.905	0.232
IP_{12}	2	4	2:20	2:00	1:40	3:30	15:40	5:02	2:20	5:59	4.162	4.205	0.132
		mean	4:05	3:30	3:34	3:33	11:42	5:17	-	-	4.930	-	-
		median	2:40	3:30	2:35	3:30	11:35	-	3:30	-	-	4.381	-
		SD	3:20	1:10	2:23	1:47	4:08	-	-	4:13	-	-	1.911

SC also requires more storage or memory space for a database to locate a host than our proposal. In addition, AX-SC cannot support network equipment produced by other than ALAXALA Networks Corporation while our proposal can also support multiple makers. AX-SC cannot then handle the case where there is a router operated only by a user or a department between a suspicious host and a switch.

There are also many security or network vendors such as Kaspersky, F-Secure, Symantec, TrendMicro, Paloalto, FireEye, Fortigate and Cisco that provide systems to isolate a suspicious host. Their systems, however, assume that all network equipment is produced by the same maker, and seems to employ a traditional method using SNMP.

7. Concluding Remarks

This paper has presented automation and orchestration of an initial computer security incident response. The proposed automation and orchestration has appeared to dramatically shorten time which is necessary for an initial incident response. Our system has appeared to be able to locate and isolate a suspicious host within 10 seconds right after an IP address of a suspicious host is given. Right after an external organization alerts an event and we recognize, we have been able to isolate a suspicious host within 1 minutes. We are now considering to identify a responsible person, e.g., a user, of the suspicious host when locating the host.

References

[1] Tor Project: Tor Project: Anonymity Online, `https://www.torproject.org/` (2002). Accessed: 2017/06/03.

[2] LAC Co., Ltd: Japan Security Operation Center(JSOC®) — Services and Products — LAC Co., Ltd., `https://www.lac.co.jp/english/service/operation/jsoc.html` (1995). Accessed: 2017/05/26.

[3] National Institute of Informatics: National Institute of Informatics, `http://www.nii.ac.jp/` (2007). Accessed: 2017/05/26.

[4] Plummer, D.: Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware, RFC 826 (Standard) (1982). Updated by RFCs 5227, 5494.

[5] Microsoft: [MS-SMB]: Server Message Block (SMB) Protocol, `https://msdn.microsoft.com/en-us/library/cc246231.aspx` (2017). Accessed: 2017/06/25.

[6] ALAXALA Networks Corporation: AX-Security-Controller, `http://www.alaxala.com/jp/news/press/2017/20170601.html` (2017). Accessed: 2017/06/03.

[7] OHMORI, M.: On a SNMP DoS Attack against Vulnerable Architecture of Network Equipment, *SIG Technical Reports*, Vol. 2016-IOT-33, No. 4, pp. 1–4 (2016).

[8] IEEE Std. 802.1ab-2004: *Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks: Station and Media Access Control Connectivity Discovery* (2004).

[9] NAGAI, Y., TADAMURA, K. and OGAWARA, K.: Considering Incident Management Systems in Some National Universities, *SIG Technical Reports*, Vol. 2014-IS-127, No. 7, pp. 1–7 (2014).

[10] Software, E.: The Trac Project, `https://trac.edgewall.org/` (2003). Accessed: 2017/05/19.

[11] Hasegawa, H., Yamaguchi, Y., Shimada, H. and Takakura, H.: A Countermeasure Support System against Incidents caused by Targeted Attacks, *Journal of Information Processing*, Vol. 57, No. 3, pp. 836–848 (2016).