Featured Articles

Work on Cybersecurity Measures for Collaboration between Organizations

Masato Terada, Dr. Eng.
Masashi Fujiwara
Akiko Numata
Yukari Nishikawa
Ruiko Kuba

OVERVIEW: Cyber-attacks continue to evolve, with a growing diversity of security incidents due to attacks and severe consequences for social infrastructure built using the Internet and based on information systems and control systems. In addition to leading cybersecurity countermeasures at Hitachi through its incident operations work, the HIRT is also working on a new problem-solving approach to cybersecurity measures whereby it seeks to obtain an overview of malicious activity by sharing information with CSIRTs at other organizations.

INTRODUCTION

LOOKING back, 2014 was a year for rethinking measures for countering vulnerabilities, including Heartbleed, Shellshock, and Padding Oracle On Downgraded Legacy Encryption (POODLE). These are names for different vulnerabilities that attracted attention because of their widespread impact. These vulnerabilities made it clear that social infrastructure built using the Internet and based on information systems and control systems is confronted with the challenges they pose as threats with the potential to lead to security incidents. They also demonstrate the need to deal, through daily work on cybersecurity measures, with the challenges posed by vulnerabilities with the potential to become new threats.

The Hitachi Incident Response Team (HIRT) helps provide safe social infrastructure and keep customers and other parts of society secure by protecting Hitachi as a whole from potential security incidents resulting from new threats and by responding promptly if an incident does occur. This article describes the HIRT's work on cybersecurity measures for collaboration between organizations.

TRENDS IN SECURITY INCIDENTS

Overview

The nature of cyber-attacks using malware continues to undergo major changes as the technology evolves. Around 1999, this included viruses sent as e-mail attachments; around 2001, there were network worms that exploited vulnerabilities; and around 2004, remotely controlled bots were being circulated. Web-based infections that exploited vulnerabilities in the plugins or other applications used by browsers began appearing around 2008, and 2011 saw the emergence of targeted attacks that combined e-mail and remote control tools to break into organizations' internal networks. The infection mechanisms used by malicious activity have broadened in step with the available communications infrastructure, including e-mail, web access, and social networks.

One of the topics of cybersecurity in 2014 was the emergence of the problem of vulnerabilities that pose threats with the potential to cause various security incidents involving social infrastructure (see Table 1). Among the characteristics of security incidents are the increasingly serious damage caused by malicious

Table 1. Typical Examples of Vulnerabilities Reported During 2014
Here "vulnerability" means the security defects that have the potential to cause a loss of performance or other functionality in the event of an attack such as unauthorized access or malware.

Date	Summary of vulnerabilities
April 2014	Heartbleed OpenSSL* issue
September 2014	Shellshock Bash issue
October 2014	POODLE SSL 3.0 issue
January 2015	GHOST GNU C Library (glibc) issue
March 2015	FREAK Export-grade RSA key issue

SSL: secure sockets layer
POODLE: padding Oracle on downgraded legacy encryption
FREAK: factoring attack on RSA-EXPORT keys
* OpenSSL is a registered trademark of the OpenSSL Software Foundation, Inc.

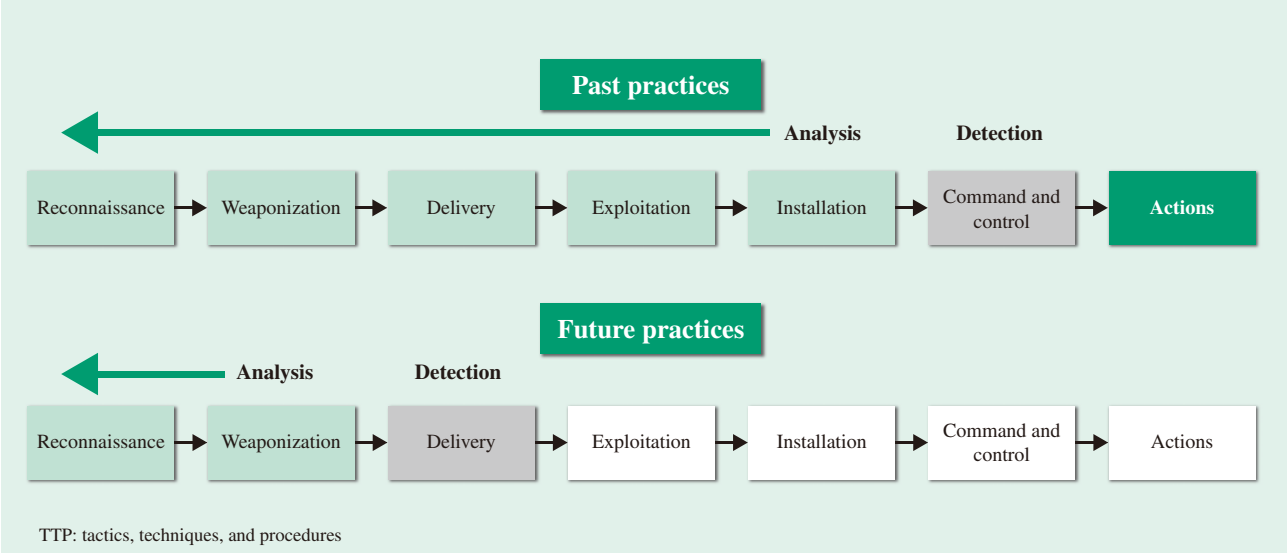

Fig. 1—Undertaking Countermeasures at an Early Stage.
The top row shows the past practices and the bottom row shows how countermeasures will be handled in the future. Future practices will include detection during the delivery stage and analysis during the weaponization stage or earlier, and a need for campaign analysis to identify the attacker's intentions and behavior patterns, actions, and TTPs.

programs that target Internet banking, and the fact that cases of damage caused by malware-based cyber-attacks, such as targeted attacks or website intrusions, have become routine. In the case of cyber-attacks against websites, in particular, password list attacks have become commonplace. These attacks involve the creation of a database of account information that can be used to attempt unauthorized login to numerous sites. There has also been a rise not just in cyber-attacks on their own, but also a rise in malicious activity in which the attacker demands money in exchange for halting an attack, such as a denial of service (DoS) amplification attack that exploits the amplification of request/response messages, and ransomware that holds personal computer (PC) files for ransom. Ransomware is the general name for malicious programs that encrypt files on a PC and then demand money in return for decrypting them. Because of the potential for ransomware to encrypt important business files and to directly impact business continuity, measures for preventing cyber-attacks now need to deal with the destruction of information as well as its exploitation.

Modeling of Cyber-attacks

To counter cyber-attacks that are becoming more diverse and ingenious, attempts are being made to investigate countermeasures by modeling this activity. In the case of targeted attacks, for example, which involve malicious activity that is both targeted (chooses a method that suits the organization being attacked) and covert (uses the organization's internal network as the platform for the attack), there are models that consider the stages in this process[1, 2]. Hutchins et al.[2] proposed a "cyber kill chain" that applies the find, fix, track, target, engage, and assess (F2T2EA) "kill chain" concept of the U.S. Air Force to cyberspace in order to model attacks from a countermeasures perspective (see Fig. 1). This model includes seven stages: reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions. It also notes the need for measures that target the early stages of an attack through detection in the delivery stage or analysis of the weaponization and earlier stages, and for campaign analysis to clarify the attacker's intentions and behavior patterns, actions, and tactics, techniques and procedures (TTPs).

Along with modeling the stages of a cyber-attack, how to use information for campaign analysis is also a subject of study. The structured threat information expression (STIX) language[3] developed by The MITRE Corporation of the USA is an extensible markup language (XML) specification for describing the process of a cyber-attack from the attack to the countermeasures. Work on the specification began with the exchange of information about attacks between the United States Computer Emergency Readiness Team (US-CERT) and the CERT*/Coordination Center

* CERT is a registered trademark of Carnegie Mellon University.

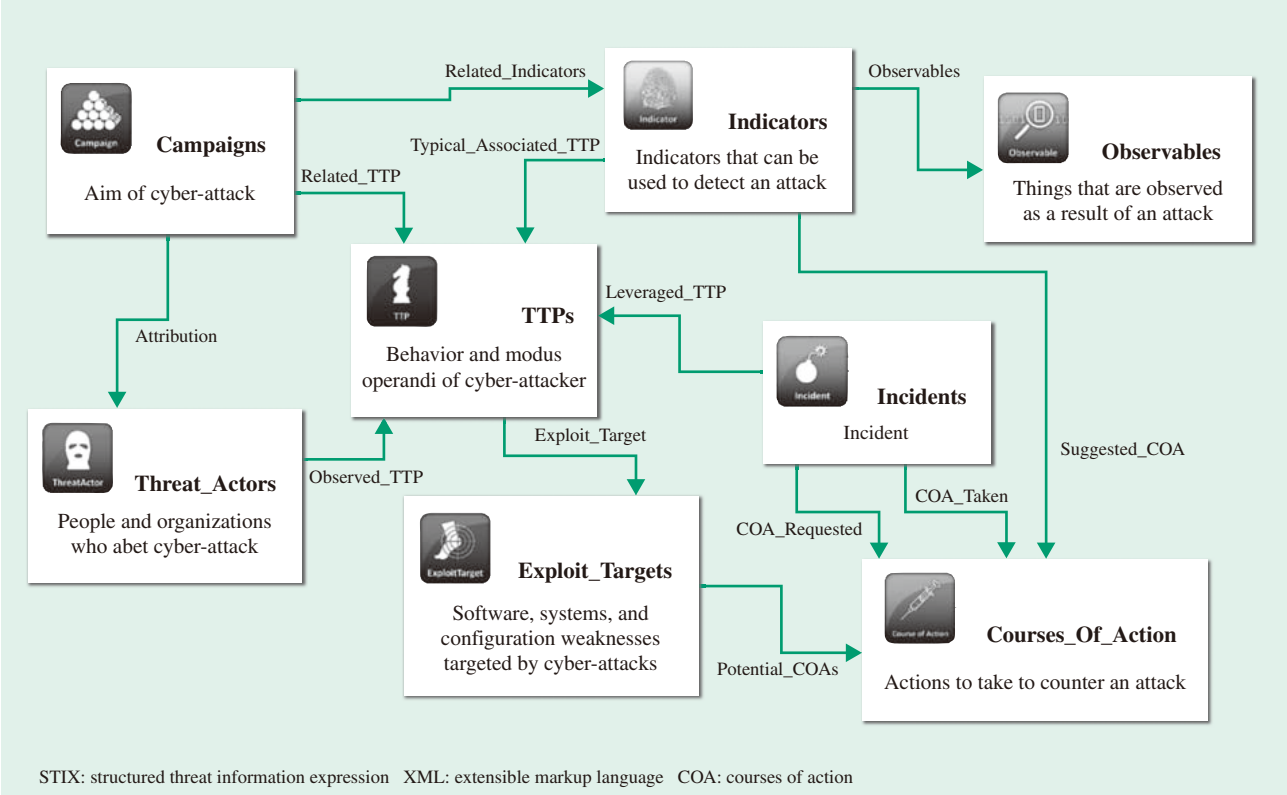

Fig. 2—Use of STIX to Define Structure of Threat.
STIX is an XML specification for describing the process of a cyber-attack from the attack to the countermeasures.

(CERT/CC) in 2010, and the release of version 1.0 in April 2013. STIX aims to establish the structure of cyber-attacks in order to link together not only the circumstances for detecting cyber-attacks, namely the software, systems, and configuration weaknesses targeted by cyber-attacks, but also the behavior and modus operandi of attackers and the people and organizations who abet cyber-attacks (see Fig. 2).

This modeling and structural analysis of cyber-attacks has attracted attention as a way for organizations to work together on cyber countermeasures through the sharing of information on "observables" (things that are observed as a result of an attack) and "indicators" (things that can be used to detect an attack), and attempts are underway to apply it at various sites.

HITACHI CSIRT ACTIVITIES

CSIRT

Interest in Computer Security Incident Response Teams (CSIRTs) and the functions performed by CSIRTs has grown in Japan since 2012. One of the main activities of these teams is incident response, meaning responding to any incidents that occur in accordance with a predetermined plan that was devised through the sharing of information about the causes of incidents and how to respond to them. Up until around 2005, seeking to resolve problems by having CSIRTs belonging to different organizations inform each other about their practices was an effective approach to incident response. However, the changing nature of cyber-attacks and other security incidents influenced the thinking of those whose job it was to respond, leading to calls for CSIRTs from different organizations to resolve problems by working together to obtain an overview of malicious activity. This meant there was a need to adopt the higher level approach of cyber-attack campaign analysis in order to counter cyber-attacks that were becoming more diverse and ingenious (see Fig. 3).

HIRT

HIRT commenced operation in April 1998 as a research project for establishing a CSIRT for Hitachi. This work included setting the requirements for HIRT to function as a CSIRT, namely, establishing capabilities for "predicting and adjusting to threats from a technical perspective," "conducting technical collaboration activities," and "liaising with external communities on technical aspects" when engaged

in activities such as countering vulnerabilities and responding to incidents. HIRT's mission is to draw on its experience in incident operations (the security actions taken to predict and prevent the damage caused by an incident and to minimize the spread of damage once an incident has occurred) to "catch any signs of future threats and take action as early as possible." Given these capabilities and mission, HIRT has the role of acting as a point of contact for CSIRT matters on behalf of Hitachi.

To counter cyber-attacks that are becoming more diverse and ingenious, HIRT is engaged in dynamic observation focusing on attacker identification ("attribution") to use observations of attacker actions in the campaign analysis of cyber-attacks.

DYNAMIC OBSERVATION FOCUSING ON ATTACKER ATTRIBUTION

Objective

In the field of cyber-attacks, "attribution" means determining the identity or location of an attacker or an attacker's intermediary[4]. To date, the static and dynamic analysis of examples of malware has focused on malware behavior. For example, the emphasis has been on things like determining the presence of functions such as C2 server connections, information theft, and backdoors, and assessing their behavior, with few instances of performing assessment or other analyses in terms of the attacker's actions, such as which of these functions the attacker used. In many cases, the response has involved static and dynamic analysis based on the assumption that the actions of the attacker and the behavior of the malware are the same thing. In the case of campaign analysis of targeted cyber-attacks involving malicious activity aimed at organizations' internal networks, however, as noted in relation to defining the structure of cyber-attacks, it is necessary to keep in mind the existence of the attacker. Accordingly, as part of the attribution process, the dynamic observation of activity aims to characterize threats in terms of the attacker's actions by considering not only malware behavior but also what actions the attacker performed, what sort of files were accessed, and so on.

Behavior Observable System

For the dynamic observation of activity, Hitachi has set up an observation environment that simulates in-house networks (see Fig. 4). This environment is a system for observing cyber-attacks launched against an organization's internal networks by an attacker

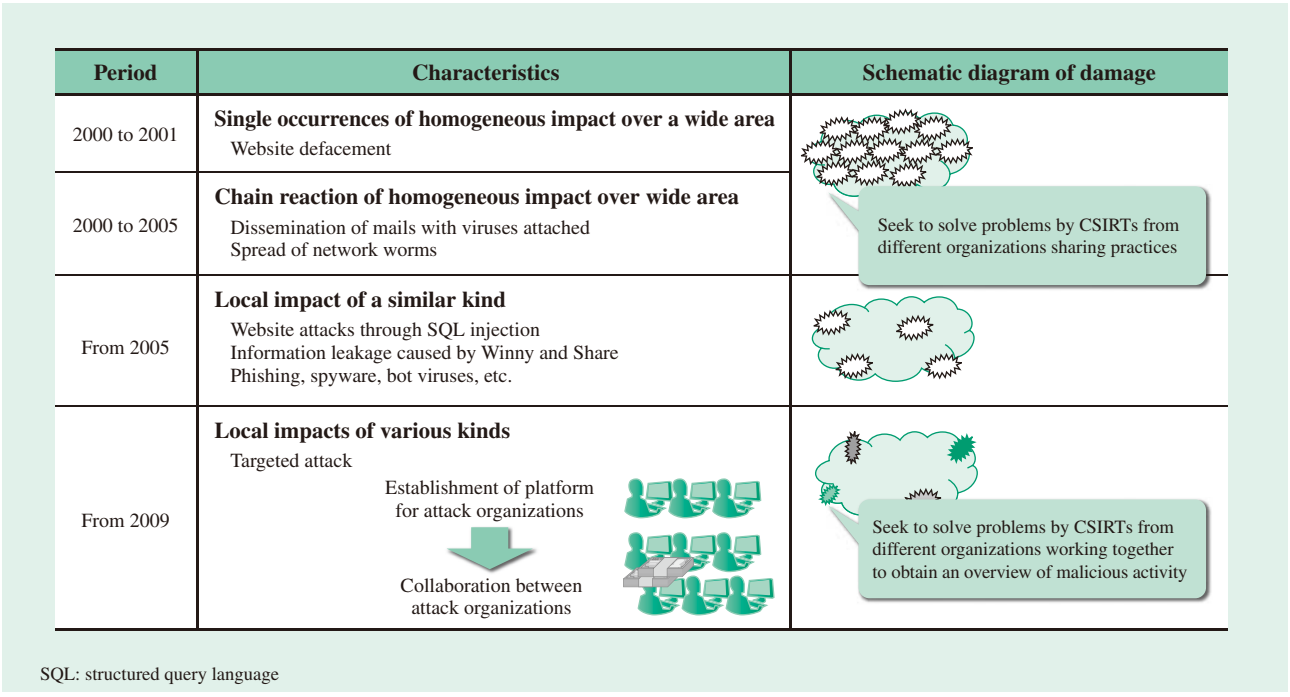

Fig. 3—Evolution of Security Incidents and Cyber-attacks.
Because of the changing nature of security incidents and cyber-attacks, collaboration between the CSIRTs of different organizations is shifting from an approach based on seeking to overcome problems by sharing practices to one based on seeking to overcome problems by obtaining an overview of malicious activity.

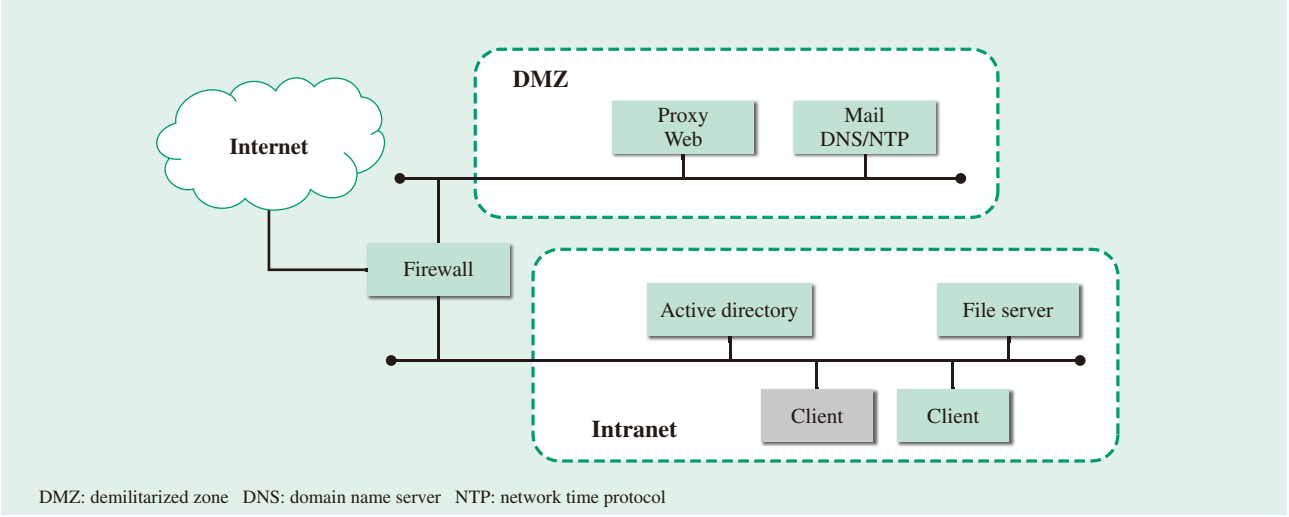

Fig. 4—Overview of Behavior Observable System.
The behavior observable system provides an environment that simulates an organization's internal network and can be used to observe the progress of cyber-attacks launched in the internal network by an attacker.

on the Internet and is intended for looking at what happens from the point when a PC on the internal network becomes infected by malware (in other words, the exploitation stage in the model of the stages of a cyber-attack). The client is a PC that executes a malware program received as an e-mail attachment (targeted attack), and is able to access the real Internet either with or without a proxy.

Example Observations

This describes observations made of a fake e-mail sent out in mid-September 2014 that claimed to be a medical bill. The fraudulent e-mail, which was made to look like the billing e-mails sent by health insurers and other agencies, attempted to infect user PCs with a malicious program ("Emdivi") that could control the PC remotely.

The file attached to the medical bill e-mail contained a malicious program that was presented as a document icon despite being an executable. On the observation system, an attacker started engaging in malicious activity approximately seven hours after the PC became infected, with a total of three hours of activity spread over three periods occurring during the 12 days until the activity ceased. The observed activity included viewing system configuration and directory information and stealing files from the infected PC and elsewhere (see Fig. 5).

While this dynamic observation of activity was only at the prototype stage, by providing information on the actions of the attacker and the nature of cyber-attacks, Hitachi believes it has the potential for uses such as cyber-attack campaign analysis and countermeasures against targeted attacks.

Involvement with anti-Malware engineering WorkShop

Dynamic observation also has another purpose, which is to enable CSIRTs from different organizations to work together to resolve problems by sharing information and obtaining an overview of malicious activity.

To achieve this, Hitachi is sharing information through the organizational committee of the anti-Malware engineering WorkShop (MWS) set up by the Computer Security Group of the Information Processing Society of Japan in the form of the Behavior Observable System (BOS), a research dataset of communication and process data collected through the dynamic observation of malware activity. By making datasets available for research use, the sharing of research results, and providing a venue for mutual assistance, the MWS acts as a place where practices can be developed and provides a framework for action based on a cooperative community of industry, academia, and government for fostering researchers, engineers, and practitioners with knowledge of malware.

CONCLUSIONS

While damage continues to occur from known threats, damage is also resulting from the emergence of new threats from cyber-attacks. Recognizing this state of affairs, HIRT seeks to implement countermeasures quickly as part of the process of identifying new threats.

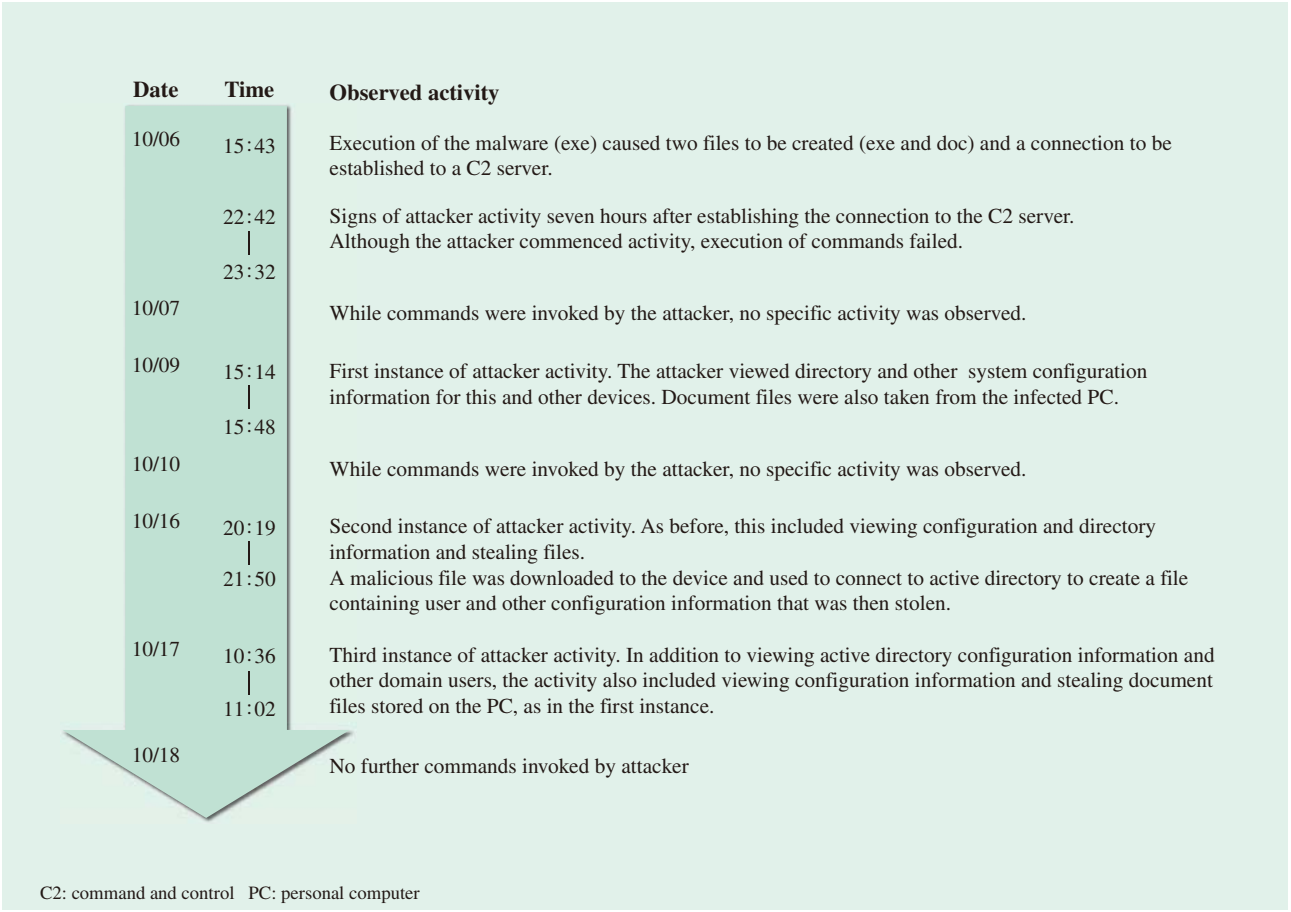

Fig. 5—Example Observations Using Behavior Observable System.
In a total of three hours of activity spread over three periods occurring during the 12 days until activity ceased, the attacker engaged in activities that included viewing system configuration and directory information and stealing files from the infected PC and elsewhere.

With respect to implementing countermeasures in particular, Hitachi aims to take the initiative in having CSIRTs from different organizations work together to resolve problems by sharing information and obtaining an overview of malicious activity. Specifically, this means countering cyber-attacks through the sharing of information by collaboration between organizations using "observables" (things that are observed as a result of an attack) and "indicators" (things that can be used to detect an attack) based on modeling that considers the different stages of a cyber-attack and defining the structure of attacks.

Hitachi also aims to contribute to making social infrastructure safe and secure through involvement in training of personnel in the academic sector to foster the next generation of the CSIRT community, including MWS.

ACKNOWLEDGMENTS

The dynamic observation of activity was conducted under contract with a field experiment project run by the Ministry of Internal Affairs and Communications to practice exercises for the analysis of and practical models for defense against cyber-attacks. The authors wish to express their sincere gratitude for the valuable advice and assistance received while conducting the dynamic observation of activity.

REFERENCES

(1) Information-technology Promotion Agency, Japan, "Overview of System Design Guide for Sophisticated Targeted Attacks," (Sep. 2014), https://www.ipa.go.jp/security/vuln/newattack.html in Japanese.
(2) E. M. Hutchins et al., "Intelligence-driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," (ICIW2011) (Mar. 2011).
(3) STIX, http://stixproject.github.io/
(4) D. A. Wheeler et al., "Techniques for Cyber Attack Attribution," Institute for Defense Analysis, IDA Paper (Oct. 2003).
(5) "anti-Malware engineering WorkShop 2015 (MWS2015)," http://www.iwsec.org/mws/2015/en.html

ABOUT THE AUTHORS

Masato Terada, Dr. Eng.
Hitachi Incident Response Team, Strategic Cybersecurity Business Planning Department, Cloud Services Division, Information & Telecommunication Systems Company and Center for Technology Innovation - Systems Engineering, Research & Development Group, Hitachi, Ltd. He is currently engaged in CSIRT collaboration activities for the incident operation of cyber security. Dr. Terada is a member of the Information Processing Society of Japan (IPSJ).

Akiko Numata
Hitachi Incident Response Team, Strategic Cybersecurity Business Planning Department, Cloud Services Division, Information & Telecommunication Systems Company, Hitachi, Ltd. She is currently engaged in the establishment of an internal education framework for vulnerability handling and incident response.

Ruiko Kuba
Hitachi Incident Response Team, Strategic Cybersecurity Business Planning Department, Cloud Services Division, Information & Telecommunication Systems Company, Hitachi, Ltd. She is currently engaged in applying the STIX approach to the sharing of information regarding cyber threats.

Masashi Fujiwara
Hitachi Incident Response Team, Strategic Cybersecurity Business Planning Department, Cloud Services Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in vulnerability handling and incident response for Hitachi products and Internet application services.

Yukari Nishikawa
Hitachi Incident Response Team, Strategic Cybersecurity Business Planning Department, Cloud Services Division, Information & Telecommunication Systems Company, Hitachi, Ltd. She is currently engaged in information sharing of cyber threats for CSIRTs.