Incident Response Solution to Minimize Attack Damage

OGUCHI Kyohei, YAMAZAKI Teru, YAMANE Masato

Abstract

It is said that it is impossible to avoid security incidents no matter how many cyberattack countermeasures are taken. However, the possibility of mitigating the damage caused by cyberattacks depends greatly on the quality of the response taken initially, from immediately after the detection of an incident to a temporary calming down of the situation. This paper discusses the optimum form of the incident response to be taken, based on actual events. A first response support service provided by NEC is also introduced.

Keywords

cyberattacks, incident response, digital forensics, CSIRT, first response

1. Introduction

Cyberattacks that steal the information assets of enterprises and organizations or obstruct their operations for the purpose of financial gain or political abuse are increasing. In a case intended to cause serious damage to an organization, such as a leak of confidential information or a security breach, the attacker will follow a certain procedure after the malware infection is accomplished. This will include a communication to the attacking server, taking over internal authority and a search for confidential information. This means that the key to containing the damage caused by a cyberattack lies in discovering an attack at an early stage and adopting a rapid response to the incident.

In this paper, we discuss how to adopt a prompt incident response by introducing site issues and some actual cases of responses (**Fig. 1**).

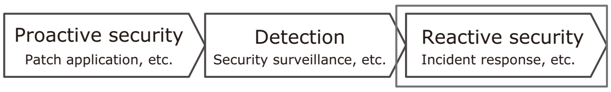


Fig. 1 Range of response measures introduced below.

2. Present Status of Incident Response

In 2015, the Japanese Ministry of Economy, Trade and Industry established the Cybersecurity Management Guidelines jointly with the Information Processing Promotion Agency, Japan. The “10 Important Items” that the management should direct their CISO (chief information security officer) to observe are as recommended in the Guidelines. These include “When facing a cyberattack, prevent further damage by taking prompt first actions and to this end, establish a Computer Security Incident Response Team (CSIRT) while at the same time developing a first action manual” in one of the ten directions.

These guidelines and the actual increase in cyberattacks are increasing the number of organizations that are studying the enhancement of their incident response procedures. However, many of them face the three issues described below that affect their incident response experience.

2.1 Loss of Evidence Due to an Inappropriate First Response

When a security staff notices an irregularity, including “finding by antivirus software or a gateway type detection product,” “execution of suspicious file, incapability of opening a file or incapability of login,” “notification from an external institution,” then various actions should be executed in order to deal with the situation. These actions such as elimination/isolation of detected files, full scanning with antivirus software and rebooting the targeted equipment are attempts to identify the source of the trouble or to prevent further damage, may sometimes turn out to be effective.

However, the incident may not be dealt with satisfactorily, which means that a potentially serious malfunction is identified. There are sometimes cases in which the actions taken for investigation and response would have previously overwritten the command/program execution history and file/folder change history, thereby causing the loss of precious clues. If the details of investigations and operations executed by the person in charge of security are not recorded, it becomes difficult to tell whether a history is recorded during the investigation or response, or that the result of the executed attack, and the investigation gets more difficult in such a case (**Fig. 2**).

2.2 Resource Insufficiency of Digital Forensic Engineers

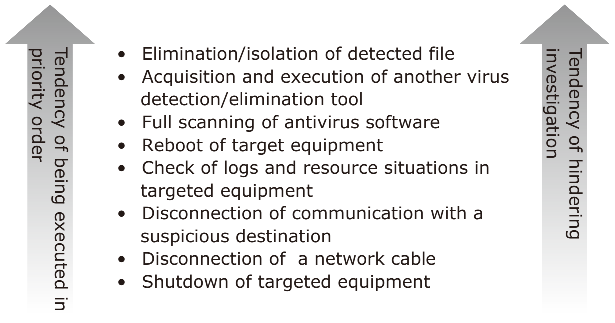
Technology for analyzing computers, servers and networks in order to identify the cause of an incident and the details of the damage is called “digital forensics” (hereinafter simplified to “forensics”). The entire market suffers from an insufficiency of forensic engineers. Business incident responses are thereby not only incapable of building optimum systems in support of user enterprises and organizations but they are also even unable to help client organizations that need support due to an actual occurrence of incidents.

This inadequacy is due to the need for the advanced knowledge of forensic engineers. In order to find traces left on a computer, a knowledge of the internal operations and principles of computers such as file systems and memory architectures is required. Such tasks are inherently difficult for humans to perform satisfactorily. On the other hand, developments in the IT industry are generally shifting towards an environment that uses high-level languages that are relatively easy to understand for humans. Therefore, the opportunities for learning technologies based on the principles of computers are becoming very rare. Such a background increases the scarcity of human resources that are capable of dealing competently with an incident response. This situation causes a serious insufficiency in the supply of forensic engineers compared to the demand (**Fig. 3**).

2.3 Environments in Which the Person in Charge Cannot Focus Exclusively on an Incident Response

When a company does not have forensics engineer, it must ask for the immediate support of experts from outside the company. However, as described above, depletion of resources over the entire market makes it necessary to contact several service sources in order to find suitable support that is available immediately. Furthermore, few organizations prepare a sufficient amount of their budgets to deal with incidents that are unpredictable. Consequently, the person in charge of the incident response must perform operations that are not directly associated with it. These will include requests for proposals, investigation of the proposal details and in-house decisions regarding special budget allocations (**Fig. 4**).

In fact, even serious situations cannot always be understood. It is in general extremely difficult to obtain clear understanding and consent of managements that are not security experts, by merely showing only the signs of potential threats (**Fig. 5**). As a result, in many cases persons in charge tend to take a long time over a response because of an inability in obtaining the re-


Tendency of being executed in priority order
Tendency of hindering investigation

- Elimination/isolation of detected file
- Acquisition and execution of another virus detection/elimination tool
- Full scanning of antivirus software
- Reboot of target equipment
- Check of logs and resource situations in targeted equipment
- Disconnection of communication with a suspicious destination
- Disconnection of a network cable
- Shutdown of targeted equipment

Fig. 2 Actions that tend to be executed in priority order and their effects on investigation.

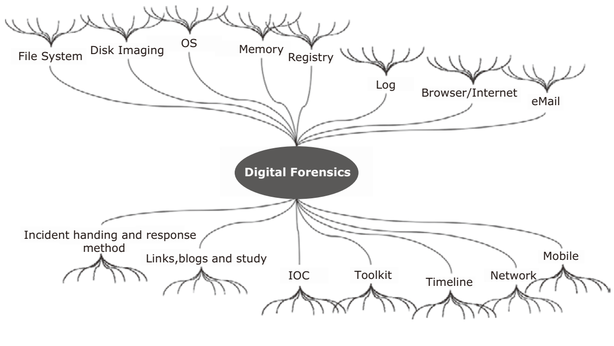


Fig. 3 Image of technological elements required by forensics[1].

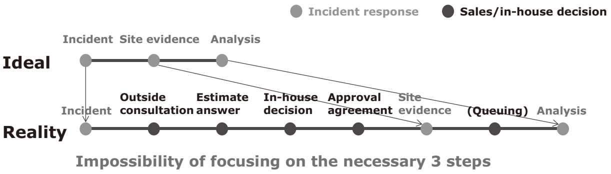


Fig. 4 Examples of indirect operations imposed on the person in charge.

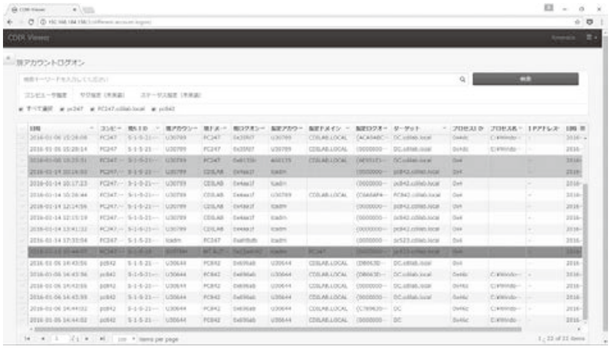


Fig. 5 Example of cyberattack traces available in a first response (Traces indicating the potential of an account acquisition by an attacker).

quired support at required timings. Usually, if a long time is available to the attacker, the violation can be extensive and the traces of attacks will be hidden and the investigations become increasingly complex. Additionally, in such a case, some cyberattacks change the hashes and communication destinations of malware in use for every infected terminal. Once the malware has spread because of an erroneous first response, repair will become extremely difficult because of the differences in the infection detection conditions between each piece of the malware.

3. Issue Solution Methods

In section 2 above, we mentioned the following three issues of incident response;

1) Loss of evidence due to an inappropriate first response;
2) Difficulty in securing forensic engineers;
3) Impracticality of the person in charge focussing exclusively on an incident response.

The following subsections will describe the methods of solving these issues.

3.1 Appropriate and Rapid Site Evidence Preservation

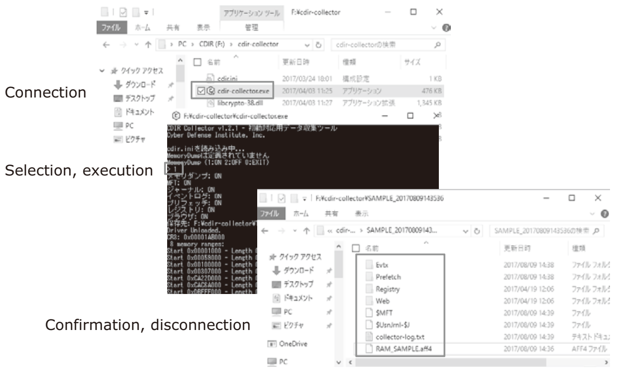
An effective method for mitigating serious damage is to adopt the action of "preservation of data in the terminals that might be attacked" at an early stage of a first response to a cyberattack. This is because preserving the necessary data increases the potential of clarifying what has actually happened when detailed investigations become necessary.

However, because an insufficiency of information immediately after discovery of an incident makes it hard to judge both the kind of and the amount of data to be preserved, the preservation work is often postponed in consideration of the amount of labor required by it. This results in one of the currently discussed issues, which in many cases is the loss of evidence. The Cyber Defence Institute Inc. (CDI), which is a security-dedicated company of the NEC Group, has developed a tool called the CDIR Collector that enables the preservation of data suitable for an incident response. This tool selects the targets of preservation by considering the balance between the volatility and the value of the information (**Table**).

When this tool is incorporated in a USB memory stick

Table Data preserved by CDIR Collector and the information available from it.

Preserved data	Available information (Examples)	Usage in analysis(Examples)
Memory	Information on recent activities, file cache and communication destinations	• Suspicious communication destinations • Finding of (running) programs • Investigation of related files
Metadata	File paths, filenames, file timestamps	• Identification of file creation (installation) date/time • Attached information on suspicious files
Journal	File/folder modification log	• Discovery of malware • Occurrence of information theft
Event log	Situations of local account logon/logoff, service/task schedule processing and system operations	• Investigation of scope of damage • Presence of suspicious services/tasks
Prefetch	Program execution time/dates and count, file paths,and related files	• Discovery of malware, investigation of its storage location • Investigations of related files
Registry	Program execution history, auto run settings and hash values	• Discovery of malware (or judgment of malware) • Presence of suspicious auto run settings
Browser history	Websites accessed	• Identification of source and date/time of infection



F:¥cdir-collector

名前	更新日時	種類	サイズ
cdir.ini	2017/03/24 18:01	構成設定	1 KB
☑ cdir-collector.exe	2017/04/03 11:25	アプリケーション	476 KB
libcrypto-38.dll	2017/04/03 11:27	アプリケーション拡張	1,345 KB

F:¥cdir-collector¥cdir-collector.exe

```
CDIR Collector v1.2.1 - 初動対応用データ収集ツール
Cyber Defense Institute, Inc.

cdir.iniを読み込み中...
MemoryDumpは定義されていません
MemoryDump (1:ON 2:OFF 0:EXIT)
> 1
メモリダンプ: ON
MFT: ON
ジャーナル: ON
イベントログ: ON
プリフェッチ: ON
レジストリ: ON
ブラウザ: ON
保存先: F:¥cdir-collector¥
Driver Unloaded.
CR3: 0x00001AB000
 8 memory ranges:
Start 0x00001000 - Length
Start 0x00058000 - Length
Start 0x00100000 - Length
Start 0x00307000 - Length
Start 0xCA22D000 - Length
Start 0xCAC6A000 - Length
Start 0xDBFFF000 - Length
```

F:¥cdir-collector¥SAMPLE_20170809143536

cdir-... › SAMPLE_20170809143...

SAMPLE_20170809143536の検索

名前	更新日時	種類
Evtx	2017/08/09 14:38	ファイル フォル
Prefetch	2017/08/09 14:38	ファイル フォル
Registry	2017/04/19 12:06	ファイル フォル
Web	2017/04/19 12:06	ファイル フォル
$MFT	2017/08/09 14:39	ファイル
$UsnJrnl-$J	2017/08/09 14:39	ファイル
collector-log.txt	2017/08/09 14:39	テキスト ドキュ
RAM_SAMPLE.aff4	2017/08/09 14:36	AFF4 ファイル

Fig. 6 Case of execution of CDIR Collector.

or network drive, data can be preserved in a few to less than twenty minutes by connecting the targeted terminal and running the tool (**Fig. 6**).

3.2 Clarification of the Role of One's Own Organization and Those to be Outsourced

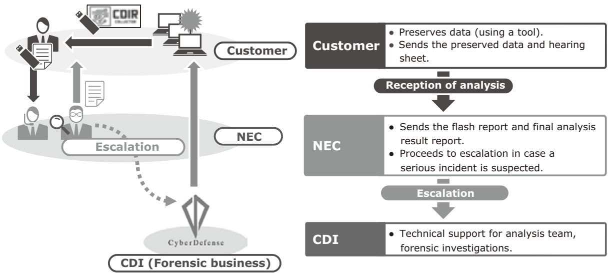
When implementing a response involving high technology hurdles to be done by one's own organization, such as via forensics, it is imperative to consider getting external cooperation in advance. What is important is to analyze the possessed operations and human resources, e.g. whether or not one's own organization has a suitable person in charge of security and a security system is maintained. Furthermore it is helpful to clarify the extent of response operations performed by one's own organization and those to be outsourced and to reserve resources for investigations and analyzes for use in case of need.

3.3 Advance Preparation and Dissemination

Smooth responses to even unexpected incidents are possible by preparing the incident response plan and the decision making process. For example, who should do what and call whom should be prepared in advance and disseminating the understanding of incidents among the organization members including the management.

4. Incident Response Support Service

Benefiting from the facilitation of the data preserved by the CDIR Collector, NEC has started a remote support service that analyzes the data preserved by the CDIR Collector (**Fig. 7**).



Customer
- Preserves data (using a tool).
- Sends the preserved data and hearing sheet.

Reception of analysis

NEC
- Sends the flash report and final analysis result report.
- Proceeds to escalation in case a serious incident is suspected.

Escalation

CDI
- Technical support for analysis team, forensic investigations.

Fig. 7 Outline of the service.

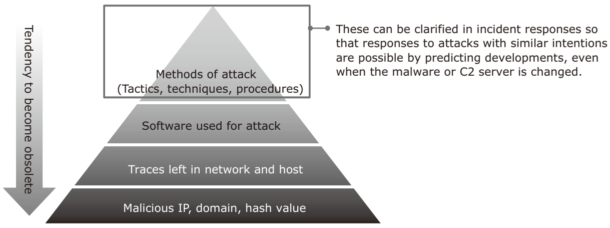

Tendency to become obsolete
Methods of attack
(Tactics, techniques, procedures)
Software used for attack
Traces left in network and host
Malicious IP, domain, hash value
These can be clarified in incident responses so that responses to attacks with similar intentions are possible by predicting developments, even when the malware or C2 server is changed.

Fig. 8 Image of knowledge obtained through service provisions.

This service consists of an analysis by NEC's special team of traces of cyberattacks remaining in terminals. Unlike the previous forensic services, it features quick first response support by setting a service target level. Specifically, it aims at issuing a flash report within one operating day after receiving the preserved data from the customer.

Should information leak or other serious damage be discovered, the team takes thorough measures in collaboration with the CDI. As the service is provided on a monthly agreement basis, it can omit clerical operations that often take excessive time over incident responses, such as for estimations and in-house decisions. This service provides a scheme for enabling the customer to swiftly implement a focussed incident response.

5. Conclusion

In the above, the authors discussed the importance of a first response to incidents and a forensics-based service for enabling a prompt response.

The incident response service provided responsibly by NEC is a solution for preventing a cyberattack incident from becoming a serious one. NEC aims to feedback knowledge quickly to the NEC Cybersecurity Group on the latest methods of attack[2)] (**Fig. 8**) and on issues in customer security operations that are clarified during the service provision. This procedure will serve the provision of improved services for all of our customers.

Reference

1) Aman Hardikar: Forensics, Mind Maps
http://www.amanhardikar.com/mindmaps/Forensics.html

2) Use of the term "Intelligence" in the RSA 2014 Expo
http://detect-respond.blogspot.com/2014/03/use-of-term-intelligence-at-rsa.html

Authors' Profiles

OGUCHI Kyohei

Assistant Manager
Security Business Promotion Office

YAMAZAKI Teru

Senior Analyst
Cyber Defense Institute, Inc.

YAMANE Masato

Assistant Manager
National Security Solutions Division

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.12 No.2 Cybersecurity

- Building Futureproof Security to Support Business Safety and Reliability -

Social trends & NEC’s approach

Cybersecurity solutions

Applications of AI technology to cybersecurity

In-house efforts provide safety and security for customers

Vol.12 No.2
January 2018

Special Issue TOP