Proactive Defense Model Based on Cyber Threat Analysis

● Takeshi Osako ● Tomoyoshi Suzuki ● Yoichi Iwata

To defend against cyber attacks, enterprises are establishing computer security incident response teams (CSIRTs) and ensuring they have defense in depth. However, such measures are not sufficient for achieving a perfect defense against attacks, and the number of security incidents is increasing day by day. It has reached the stage where, to further strengthen protection, it is necessary to implement proactive defense as well as to improve reactive defense. Each attacker tends to have unique peculiarities, and "cyber threat intelligence" can be extracted from them. Extracting this intelligence from the various signs and artifacts of attacks is defined as "cyber threat analysis." Establishing a proactive defense model based on this definition is a useful approach to detecting attacks targeting a specific organization, which have been increasing in recent years and are difficult to detect and defend against with existing security measures. This paper describes the standardization of cyber threat analysis techniques including analysis of malware and extraction of cyber threat intelligence. It also describes a model that provides proactive defense against future cyber attacks by utilizing cyber threat intelligence.

1. Introduction

The Japanese Basic Act on Cybersecurity,[1] enacted in 2014, established the Cybersecurity Strategic Headquarters, clarified points on promoting the development of a domestic security industry, and emphasized the increasing importance of security measures in cyberspace.

Cyber attacks have become increasingly sophisticated and stealthy in recent years—targeted areas have expanded, and the number of incidents (events in which servers or personal computers are breached by an attack) has increased. As a result, business enterprises and organizations have found that they cannot help but shift from an approach that attempts to prevent intrusions to one that presumes that intrusions are bound to occur. Even if an attacker breaches security, it is still important to localize the range of the damage and prevent it from spreading. It is thus generally best to adopt a defense in depth strategy that includes using advanced technologies such as "sandboxing," which enables files to be examined in an isolated environment to check for suspicious behavior. It is also helpful to set up a computer security incident response team (CSIRT) to respond to incidents as they occur.

Such measures, however, do not provide a perfect defense since damage can still occur from information leaks.[2] One reason for this situation is the appearance of the advanced persistent threat (APT), which is a repeated targeted attack customized on the basis of a detailed strategy formulated by collecting information on security measures in the targeted organization and elsewhere. This situation has motivated Fujitsu to analyze APT attacks to determine their origins, infrastructures, and techniques so that new types of countermeasures can be implemented. Fujitsu has begun activities aimed at achieving such countermeasures.

In this paper, we introduce a model for analyzing the objective, infrastructure, techniques, and tools of an attack and using those features to create a proactive defense.

2. APT attacks: countermeasures and issues

The features of APT attacks can be organized by attack phase. Typical attacks and countermeasures in each attack phase are listed in **Table 1**.[3] The attack phases are summarized as follows.

- Prepare for attack: Prepare targeted e-mails with attached malware etc. for breaching security of targeted organization; prepare command and control (C2) server
- Infiltrate: Use targeted e-mails to infect personal computers in targeted organization with malware
- Construct infrastructure: Establish backdoor; survey network environment to collect information about internal network and servers; send collected information to C2 server
- Breach and explore: Expand inter-terminal breach; breach servers; collect information
- Execute objective: Steal valuable information, destroy critical systems, etc.

The countermeasures typically applied in each phase of an APT attack have limited effectiveness as attackers have already developed techniques to avoid them, as described below.

1) Use targeted e-mails

- Countermeasure 1: Targeted e-mail training

Provide training on targeted e-mail and improve the ability of employees to recognize targeted e-mail messages.

- New attack technique: Back-and-forth e-mail exchange

After exchanging e-mails with a customer service representative of the targeted organization several times in the guise of a customer, the attacker sends an e-mail with an attached executable file containing malware to infect the representative's computer.

2) Infect computers

- Countermeasure 2: Sandbox isolation

Isolate e-mail with an attached executable file in a sandbox and check for malware by analyzing the behavior of the file.

- New attack technique: Sandbox detection

A new type of malware is used that detects virtual environments used by sandbox products and adjusts the attack so that the file exhibits no suspicious behavior and appears to be normal.

3) Establishment of backdoor and survey of network environment

- Countermeasure 3: Illicit external communications blocking

Monitor outbound communications and block detected communications exhibiting suspicious behavior.

- New attack technique: Encrypted communications

Encrypt outbound communications, preventing the features of those communications from being detected.

4) Communication with C2 Server

- Countermeasure 4: Authentication proxy implementation

Implementing an authentication proxy server blocks communications from a malware-infected device to a C2 server, thereby preventing remote operations by the attacker and information leaks.

- New attack technique: Eavesdropping to obtain authentication information

The attacker eavesdrops on the authentication proxy server to obtain authentication information and uses that information to enable communication between the C2 server and a malware-infected device via the authentication proxy server.

An attacker can thus use a variety of techniques to avoid countermeasures and inflict serious damage

Table 1
Attack phases and typical countermeasures.

Phase	Prepare for attack	Infiltrate	Construct infrastructure	Breach and explore	Execute objective
Typical actions	• Prepare targeted e-mail with attached malware etc. • Prepare C2 server	• Infect computers in targeted organization with malware	• Establish backdoor • Survey network environment • Send collected information to C2 server	• Expand inter-terminal breach • Breach servers Collect information	• Steal valuable information • Destroy critical systems
Countermeasures	• Targeted e-mail training (Countermeasure 1)	• Sandbox isolation (Countermeasure 2)	• Illicit external communications blocking (Countermeasure 3) • Authentication proxy implementation (Countermeasure 4)		

on a target through breaching and remote operations. Despite the resources expended on countermeasures to detected attacks, the effect is only temporary as attackers quickly learn how to avoid countermeasures. Countermeasures against undetected attacks that are based on attacker behavior will thus become increasingly important.

3. Cyber threat analysis and cyber threat intelligence

An APT attack is one that is mounted repeatedly with a clear-cut objective. We consider that attacks by the same attacker can reveal particular characteristics about that attacker. This means that certain characteristics may be uncovered by analyzing the signs and artifacts of such attacks:

- Features of attack infrastructure,
- Features of attack tools (malware),
- Features of attack techniques, and
- Attack objective.

Such attack-related information is defined as "cyber threat intelligence," and the process of extracting cyber threat intelligence from signs and artifacts of attacks is defined as "cyber threat analysis." Cyber threat intelligence can be used to mount a proactive defense that can infer attacker behavior, discover undetected attacks, predict potential attacks, etc. (**Figure 1**).

The following describes several cyber threat analysis techniques and associated cyber threat intelligence.

3.1 Attack channel analysis

The technique used by the attacker to infect a terminal inside the targeted organization with malware to enable remote operations is defined as the "attack channel." Attack channel analysis can best be described by the following example.

An attacker sends targeted e-mail to infect a terminal in the targeted organization with malware. This e-mail becomes the target of analysis, which, in the case of targeted e-mail, means analyzing header information, message body, and attached file(s). The following types of cyber threat intelligence can be extracted by this analysis.

- E-mail source address
- Host name, IP address, etc. of e-mail sending server
- Message subject
- Names of attached files
- Types of attached files

Another target of this analysis is a technique known as a "watering hole attack" in which the attacker tampers with websites regularly used by the targeted organization and infects them with malware.

3.2 Malware analysis

This technique analyzes malware sent by an attacker by using a three-step procedure.

1) Surface analysis

Analyze the type of file, file name, character

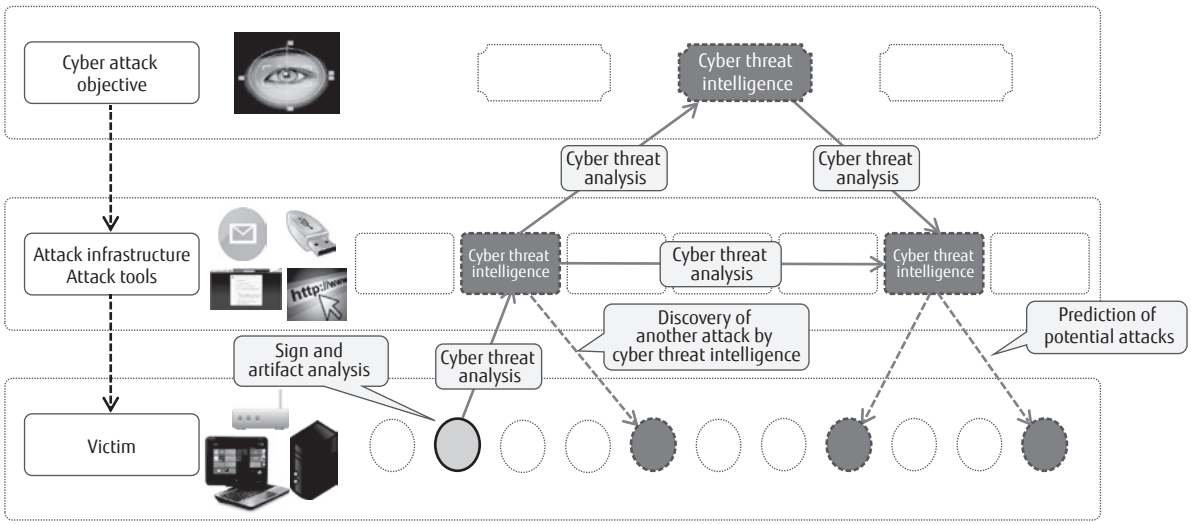

Figure 1
Proactive defense by cyber threat analysis of cyber threat intelligence.

strings within binary data, etc. without running the malware.

2) Dynamic analysis

Run the malware and analyze its behavior to determine file operation, registry operation, processes, and communications.

3) Static analysis

Reverse engineer the malware, that is, restore the compiled binary data to source code and analyze the source code to reveal detailed malware operations.

Malware analysis can yield various types of cyber threat intelligence, including

- Malware file name,
- Malware hash value,
- Files created by the malware,
- Registry key created by the malware,
- Processes initiated by the malware,
- Domain name, IP address of C2 server with which the malware communicates,
- Features of the communicated data (protocol, header information, etc.),
- Vulnerabilities exploited by the malware, and
- Malware functions (keystroke logging, execution of remote commands, etc.)

3.3 C2 analysis

This technique analyzes the C2 server to obtain various types of information.

1) WHOIS information (information about IP address and domain name registration records)

Specifically, the technique inspects WHOIS information such as domain names and IP addresses of the C2 server and identifies other servers with the same WHOIS information. These servers may also be C2 servers used by the attacker.

2) Location information

The technique analyzes the location information of the C2 server. Attackers often install a C2 server as a springboard, and such servers tend to exhibit regional characteristics.

3) Domain names, IP addresses of C2 servers (newly discovered information by passive Domain Name System [DNS] analysis)

Attackers frequently change C2 servers, so to avoid tracing, they attempt to access their C2 servers by domain name instead of by IP address. Given that domain information on a certain C2 server has been obtained, the results of queries to a DNS server in relation to that domain name can be monitored and analyzed. This process may reveal information (IP address etc.) on the attacker's next C2 server.

3.4 Attack campaign analysis

This technique uses cyber threat intelligence extracted from individual artifacts and incidents to group together those having common values. Then, if the artifacts and incidents in such a group happen to be numerous, that group is defined as a single attack campaign. Here, the artifacts and incidents included in an attack campaign are deemed to have occurred due to an attack mounted by a certain attacker with a particular objective. Once an attack campaign has been recognized, the cyber threat intelligence extracted from those artifacts may prove useful in defending against future attacks.

4. Standardization of cyber threat intelligence

Cyber threat intelligence is considered to be extremely valuable information for detecting and defending against attacks. There is therefore a need for common specifications that will enable this information to be efficiently exchanged between security systems and organizations in a systematized and near real-time manner. In response to this need, a variety of specifications have recently been released, and in this section, we introduce CybOX,[4] STIX,[5] and TAXII[6] proposed by The MITRE Corporation.

1) CybOX (Cyber Observable eXpression)

CybOX provides a format for expressing observable events. For example, the format for expressing cyber threat intelligence such as malware file names, malware startup process, and C2 server IP address would be defined in XML.

2) STIX (Structured Threat Information eXpression)

STIX provides a format for expressing cyber threat intelligence in terms of 5W1H (who, what, where, when, why, and how). This format consists of eight types of information defined in XML:

- Campaigns,
- Threat actors,
- Tactics, techniques, and procedures (TTPs),
- Indicators,
- Observables,

- Incidents,
- Courses of action, and
- Exploit targets.

3) TAXII (Trusted Automated eXchange of Indicator Information)

TAXII is a protocol for transmitting and receiving cyber threat intelligence (a vehicle for exchanging cyber threat intelligence). It enables cyber threat intelligence described by CybOX and STIX to be exchanged by a programmed process.

The MITRE Corporation has released Collaborative Research Into Threats (CRITs)[7] as an open-source system platform supporting the above standard specifications and enabling the analysis, storing, and sharing of cyber threat intelligence. On testing and evaluating CRITs, we found it to be particularly useful in several ways.

- It supports a variety of automatic tools for cyber threat analysis.
- If provides a function for extracting related information from stored data using malware information and cyber threat intelligence as search keys, which helps to simplify attack campaign analysis.
- It supports the exchange of cyber threat intelligence using CybOX, STIX, and TAXII.

5. Proactive defense model

Fujitsu's has developed a proactive detection and defense model against APT attacks that uses cyber threat intelligence.

The first step in this model is to automatically save artifacts of attack events detected by various types of sensors and logs. The next step is to perform cyber threat analysis against the stored artifacts, extract and store cyber threat intelligence, deliver that intelligence to various sensors and security information and event management (SIEM), and take an appropriate action, such as disconnecting the network containing the terminal in which an incident has occurred. This model is shown in **Figure 2**. The following defines the constituent elements of this model and explains their functions.

1) SIEM

Consolidates events from a variety of security sensors and logs from diverse information systems and assesses whether an incident has occurred on the basis of specific rules and cyber threat intelligence.

2) Incident management

Manages the priority and state of incidents and tasks that need to be executed as tickets.

3) Artifact storage

Saves artifacts of incidents (suspicious files and

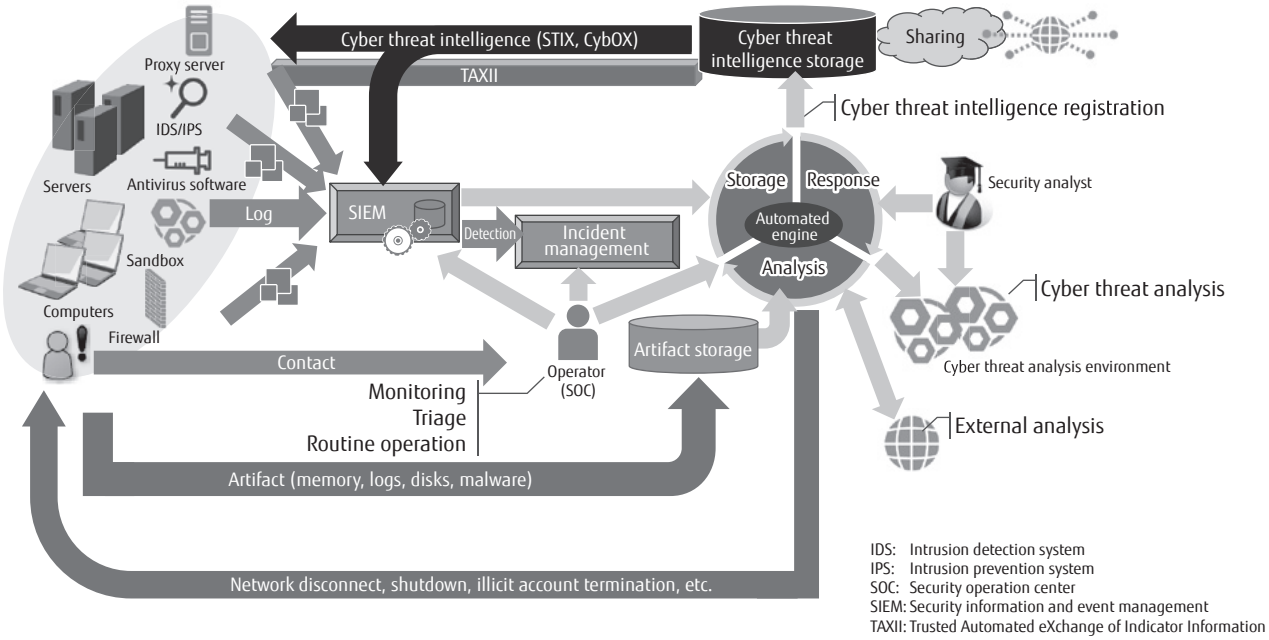

Figure 2
Proactive defense model based on cyber threat analysis of cyber threat intelligence.

logs, memory dumps, etc.) for use in automatic analysis and cyber threat analysis.

4) Automated engine

Performs the following three functions.

- Analysis

This function automatically analyzes detected events and artifacts. It searches for matches among the results of malware analysis using sandbox techniques, stored cyber threat intelligence, etc.

- Response

This function mounts a response based on the results of automatic analysis and stored cyber threat intelligence. It automatically delivers and applies cyber threat intelligence to security sensors, SIEM, etc.

- Storage

This function automatically stores cyber threat intelligence extracted from the results of analysis.

5) Cyber threat intelligence storage environment

Supports CybOX, STIX, and TAXII standards and provides a function for sharing cyber threat intelligence with diverse security sensors and organizations.

6) Cyber threat analysis environment

Analyzes threats to extract new cyber threat intelligence for proactive defense. Includes an environment for malware analysis and log analysis.

Although some of this model was implemented manually, its application was determined to have a positive effect. It showed that the use of cyber threat intelligence obtained by cyber threat analysis should make it possible to proactively defend against APT attacks. This model is also useful for automating a proactive defense to reduce the operation load.

As a future research issue, we will explore ways of extracting and using more accurate cyber threat intelligence. We also recognize that using only Fujitsu's cyber threat intelligence to deal with APT attacks is insufficient and that global collaboration with various organizations, vendors, and communities is essential.

6. Conclusion

This paper introduced a model for proactively defending against APT attacks that is based on cyber threat intelligence extracted by cyber threat analysis. It is predicted that customers' ICT environments will be subjected to an even greater variety of attacks in the future. Fujitsu plans to apply this model to the security solutions it provides to its customers to support the safe and secure operation of its customers' ICT environments.

References

1) NISC: Overview of the Basic Act on Cybersecurity (in Japanese).
http://www.nisc.go.jp/conference/seisaku/dai40/pdf/40shiryou0102.pdf
2) Verizon Enterprise Solutions: 2016 Data Breach Investigations Report.
http://www.verizonenterprise.com/verizon-insights-lab/dbir/
3) IPA: System Design Guide for Thwarting Targeted Email Attacks.
https://www.ipa.go.jp/files/000035723.pdf
4) MITRE: Cyber Observable eXpression.
https://cybox.mitre.org/
5) MITRE: Structured Threat Information eXpression.
https://stix.mitre.org/
6) MITRE: Trusted Automated eXchange of Indicator Information.
https://taxii.mitre.org/
7) MITRE: Collaborative Research Into Threats.
https://crits.github.io/

Takeshi Osako
Fujitsu Ltd.
Mr. Osako is currently engaged in the investigation of security incidents and the development of security services.

Tomoyoshi Suzuki
Fujitsu Ltd.
Mr. Suzuki is currently engaged in the development of cyber security intelligence solutions.

Yoichi Iwata
Fujitsu Ltd.
Mr. Iwata is currently engaged in the planning and development of security services.