Countermeasures against Unknown Cyberattacks Using AI

NISHINO Shinichiro, KIDA Koji, KIZU Yoshiya, YAGI Takashi, SAKAE Yoshiaki

Abstract

The spread and sophistication of cyberattacks have led to new issues when using existing security measures, such as difficulty of detection. Even when detection is successful, advanced skills and a huge amount of manpower are required to analyze the results. NEC has dealt with these issues by developing a service designed to counter the unknown cyberattacks that used to be impossible to detect by applying AI technology. This service implements "detection" of unknown attacks over the entire attack process (from malware intrusion and the spread of infection inside a system to achievement of an attacker's aim such as theft of data). After an attack "analysis" is also undertaken, thereby identifying the cause and extent of damage with a high degree of certainty. This paper introduces the current status and issues of cybersecurity, the base AI technology of the service, and its main functions and features, together with the results of the verification of how and how much the service solves the issues.

Keywords

cybersecurity, cyberattack, unknown malware, AI, lateral movement, anomaly detection, analysis, SOC, CSIRT, normal status, endpoint

1. Introduction

As recent cyberattacks are becoming more and more advanced and targeted, the number of unknown malware used in the attacks are increasing. Included are those customized from the existing malware, known malware and ones that are custom-made for each target.

In consequence, most of the pattern-matching type antivirus software that has been distributed and used widely as a typical information security measure, has almost become ineffective. This is because pattern matching is a technology for detecting known malware and was not developed against unknown malware. According to the tests conducted in-house at NEC, simply by modifying some known malware samples, the detection rate of pattern-matching type antivirus software decreased by as much as 85%.

Sandbox is a technology for detecting unknown malware. It runs a program suspected to be malware in a virtual environment isolated from the real network and determines whether or not it is a malware based on its behavior. However, malware makers have begun to counter the sandbox by implementing mechanisms for avoiding it. For example, some malware is now made not to run when it finds itself on a virtual machine.

As seen above, the approach to increasing the detection rate by identifying the malware has become a cat-and-mouse game with malware makers and it has become impossible to continue 100% detection.

Based on the situations described above, this paper introduces a service that can detect attacks by using new techniques and also improve the efficiency of analyses after detection, instead of detecting them by knowing malware in advance.

2. Issues

Malware that has bypassed the existing security measures starts activity at the endpoint (PC or server). The attacker does not send malware to the final target (database storing confidential information, etc.) directly, but utilizes an infection spreading activity called lateral movement (**Fig. 1**). The attack is thereby made via an approach from the entrance to the final target step by step in order to achieve its aim (theft of important information from the database and its transmission to the

Internet). This means that when malware penetrates a system, it is vital to detect it before actual damage is produced and to implement proper responses.

According to an independent survey by NEC, about 30% of unknown attacks bypassed the sandbox or other measures and required manual responses. This situation explains why the following two issues exist.

(1) Improving the attack detection rate

In addition to attacks by unknown malware as described above, another cause of a drop in the detection rate is by attacks that make use of the OS standard tools (Windows PowerShell, etc.). Since the OS standard tools are not malware, they are not detected by antivirus software. However, because the way they are used in an attack differs from the usual, it is necessary to detect the attack by focusing on the irregularity of their usage. Particularly important is the capability of detecting attacks across multiple endpoints (lateral movement).

(2) Improving the efficiency of response by human analysts

Attacks bypassing the detection system need to be handled manually by security analysts.

This is typically done by the SOC (Security Operation Center) / CSIRT (Computer Security Incident Response Team) as a security incident investigation. While these operations demand advanced cybersecurity skills, a huge labor input is required, such as that used in tackling the large volume of logs. In such a situation, improving the efficiency of incident response is a critical issue, because of the chronic shortage of high-level security specialists as well as the difficulty of training security experts over a short period.

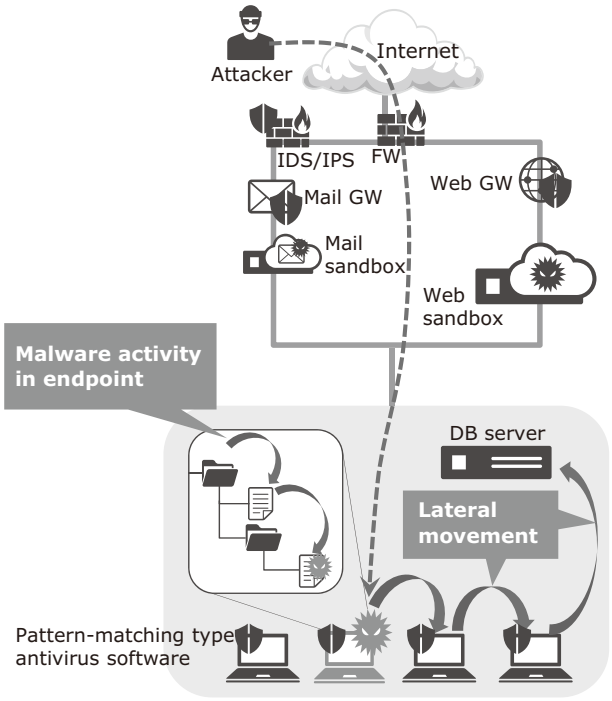


Fig. 1 Lateral movement.

3. Functions of ASI

This section introduces Automated Security Intelligence (ASI)[1) 2)], which is a self-learning type technology that detects unknown attacks using AI and improves the efficiency of the root-cause and impact analyses.

The ASI has the following two technological features (**Fig. 2**).

(1) Real-time detection of anomaly in system using AI

Firstly, the ASI collects detailed data on the operating status (program executions, file accesses, network accesses, etc.) of the entire system from

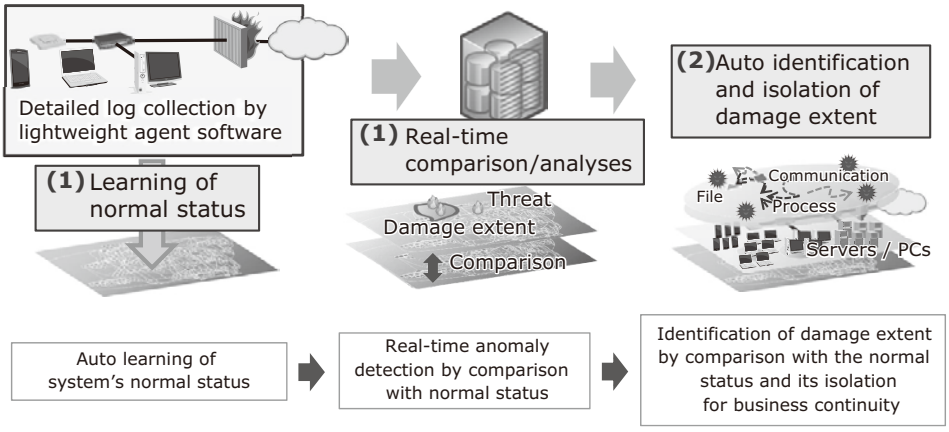


Fig. 2 Technical features of ASI.

endpoints, analyses it with AI and identifies the normal status of the system. Next, the AI is used to compare the current system status and the normal status in real time and determine a deviation from the normal status as an "anomaly."

(2) Improvement of analyses, automation of responses

As the ASI has monitored and stored the behavior in detail over the entire system, it can trace and display the series of events associated with the anomaly. This makes it possible to improve the efficiency of analyses for identifying the root-cause and impact.

Below is an explanation of the "normal status" of the system behavior, using a simple example.

Fig. 3 shows the simplified network system of an enterprise and the image of the normal status of the system. The system is composed of the following three subnetworks:

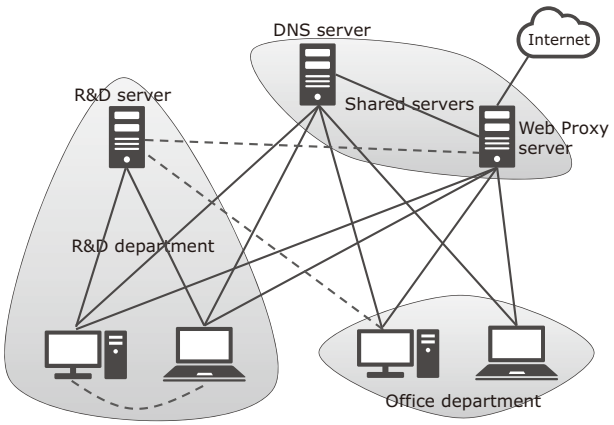


Fig. 3 Image of usual status of ASI.

1) **Shared subnetwork:**
Servers that are used commonly by the whole enterprise are deployed, such as the web proxy server.

2) **R&D department subnetwork:**
Servers and PCs used by R&D staff are deployed.

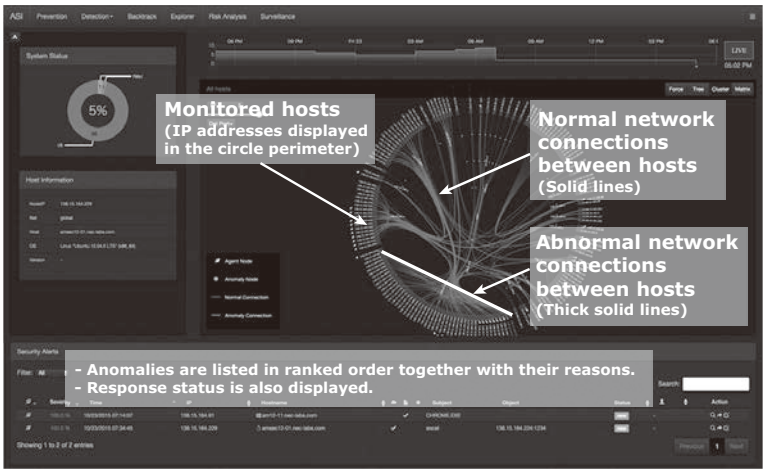
3) **Clerical departmental subnetwork:**
The PCs for the office department are deployed.

Normally, common servers are accessible by any PC in the enterprise, while the R&D servers are accessible only by the PCs in the R&D department. In contrast, it is abnormal that a computer in the office department accesses an R&D server. Such a relationship between machines is called the normal status (solid lines in Fig. 3).

When a network access that should not occur in the normal status is detected, the ASI determines that it is an "anomaly" and reports it to the administrator. Those reports will be made for cases in which a PC of an administrative department accesses a R&D dept. server, the PCs installed in the R&D department hold a direct communication between them, and an R&D server that usually does not communicate with the internet communicates with the web proxy server (broken lines in Fig. 3).

Direct connections between endpoints in the same department typically indicates lateral movements, and a connection from an R&D server to the web proxy server indicates the goal achievement phase of the attack process by malware.

Detection of a lateral movement is especially important because traditional cyberattack handling tools are designed to detect attacks in their initial malware intrusion phase or in the goal achievement phase. Once the gateway security has been bypassed, the detection of an attack is extremely difficult until it reaches the final



* As this service is still under development, the official version may differ from the example shown here.

Fig. 4 Example of anomaly detection by ASI.

phase. ASI can solve this issue because it can detect an attack even between the initial intrusion and the goal achievement, or during lateral movements, so that the chances of attack detection are increased.

Fig. 4 shows an example of an anomaly detection display of the ASI. The pie chart at the center of the right-hand display indicates the surveillance target network, solid lines indicate the normal network connections between PCs and servers, and the thick solid line indicates the abnormal (detected as anomaly) network connections.

Although the explanation in this section has been given by taking the network communications between PCs and servers as an example, ASI is capable of detecting anomalies even in a computer without network communications. This is because it learns the normal status including the program start-ups and file accesses at endpoints.

NEC is implementing the ASI service and product considering that it is not only an anomaly detection tool but that it also features the important function of improving the efficiency of identifying the infection source and damage extent of the malware and of responding to it satisfactorily. Providing ASI as a service allows it to be used even by an enterprise that does not have enough in-house security specialists.

4. Solution of Issues by ASI

This section introduces the results of verifications by applying ASI to the issues enumerated in section 2.

4.1 Issue 1: Improving the attack detection rate

(1) Unknown malware

The authors assessed the detection capabilities of ASI and other vendors' security products using AI, using malware samples which were undetectable by pattern-matching type antivirus software products. As a result, while the detection rates of the other products were 0%, that of ASI was about 80%, thereby demonstrating its high detection accuracy.

(2) Attacks making use of OS standard tools

An experiment simulating a targeted attack was conducted in a real office environment of the NEC Group. When simulated malware using OS standard commands (Windows PowerShell, etc.) was used to attack about 10 servers and about 100 computers along a realistic attack scenario including data theft, the ASI was able to detect 100% of the attacks before their goal was achieved. This experiment has verified that ASI is also effective against attacks using OS standard tools.

4.2 Issue 2: Improving the accuracy of the human response

Work that requires manual operations can be divided loosely into two categories 1) "analyses of root-cause and impact extent in case of anomaly" and 2) "handling false positives". According to an experiment completed in a real office environment of the NEC Group, the introduction of ASI has reduced the analysis period that used to take a few days per case, to 1.5 hour on average (about 5 hours max.). The number of false positives that used to be tens per endpoint per day were reduced to 0.27/endpoint/day on average. The overlapping of these two effects significantly improves the efficiency of the manual operations.

As seen in the above, unlike the previous pattern-matching and sandbox products, the ASI can detect unknown attacks and improve the efficiency of analysis after detection. This is due to fine-grained monitoring of endpoints in a real environment and AI-based analyses.

Additional features of the ASI include: detection of the spread of infection activity (lateral movements) of malware across multiple machines by integrated monitoring of multiple endpoints, providing all-in-one functions from detection to analyses as a service. ASI can also be applied as a countermeasure for insider threat as well as for malware.

In the above, the authors introduced ASI with the capability of detecting and analysing unknown attacks. In the future, NEC is planning to link ASI with other products and services and to provide solutions covering the entire process range of the SOC/CSIRT (prevention, monitoring, detection, analysis and response).

Reference

1) NEC Press Release: NEC technology uses artificial intelligence to automatically detect unknown cyber-attacks, December 2015
http://www.nec.com/en/press/201512/global_20151210_01.html
2) TAGATO Hiroki, et al.: Automated Security Intelligence (ASI) with Auto Detection of Unknown Cyber-Attacks, NEC Technical Journal, Vol.11, No.1, September 2016
http://www.nec.com/en/global/techrep/journal/g16/n01/160110.html

Authors' Profiles

NISHINO Shinichiro
Assistant Manager
Smart Networks Division

KIDA Koji
Manager
Smart Networks Division

KIZU Yoshiya
Assistant Manager
Smart Networks Division

YAGI Takashi
Assistant Manager
Smart Networks Division

SAKAE Yoshiaki
Principal Creator
Security Research Laboratories

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 -

Vol.12 No.2
January 2018

Special Issue TOP