http:d2cigre.org

CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

2015 Colloquium
October 15 to 16, 2015
Lima – PERU

D2-03_02

Introduction of Anti-malware Measures using Whitelisting based on Behavioral Detection

by

Yasuhiro Otsuka *
Kyushu Electric Power Co., Inc.
(JP)

Tadashi Kajiwara
Q-DEN BUSINESS SOLUTIONS Co., Inc.
(JP)

SUMMARY

Kyushu Electric Power Company owns a massive amount of confidential information essential to its business operations including customer information and information on nuclear power plant equipment.

To protect this confidential information from cyber attacks, so far, we have implemented anti-malware measures using blacklisting (pattern matching technique), an approach that identifies viruses by comparison with virus definition files, in order to ensure information security.

However, the dramatic increase in recent years in damage caused by cyber attacks using new types of malware undetectable by conventional measures has given rise to the need for new security measures to combat these threats.

This paper presents the background leading up to the introduction by Kyushu Electric Power Company of “anti-malware measures using whitelisting,” verification and introduction of which has been underway since FY2012, as security measures to combat new types of malware, the present state of operation of these measures and future issues to be addressed.

KEYWORDS

Virus Definition File, Pattern Matching, Targeted Attack, Vulnerability, Zero-day Attack, Anti-malware Measures using Blacklisting, Anti-malware Measures using Whitelisting.

* Postal Address of Main Author:1-82, Watanabe-dori 2-Chome Chuo-ku, Fukuoka-shi, Fukuoka, 810-8720 Japan
Fax: +81-92-761-7749 e-mail: Yasuhiro_Ootsuka@kyuden.co.jp

1. Background to Introduction

As typified by incidents of malware infection caused by targeted attacks on government organizations and defense corporations that took place in 2011, recent years have seen changes in malware types from those that target multiple unspecified users, producing flamboyant effects and exhibiting destructive behavior that make users aware of the malware infection, to those with the characteristics listed below, heightening the risk of intrusion and infection.

- Rather than reusing the types of malware that have been used in the past, new types of malware designed for specific targets or goals are created.
- New types of malware are used after verifying that they cannot be detected by general anti-malware software.
- New types of malware are created with restrictions on the environment in which they can be executed such as the inability to run anywhere but on the target computers, making them difficult to detect by third parties.

As the number of security breach incidents by new types of malware both at home and abroad increased dramatically, we needed to implement security measures to combat new types of malware as quickly as possible since we relied solely on anti-malware measures using blacklisting (pattern matching technique) provided by anti-malware software.

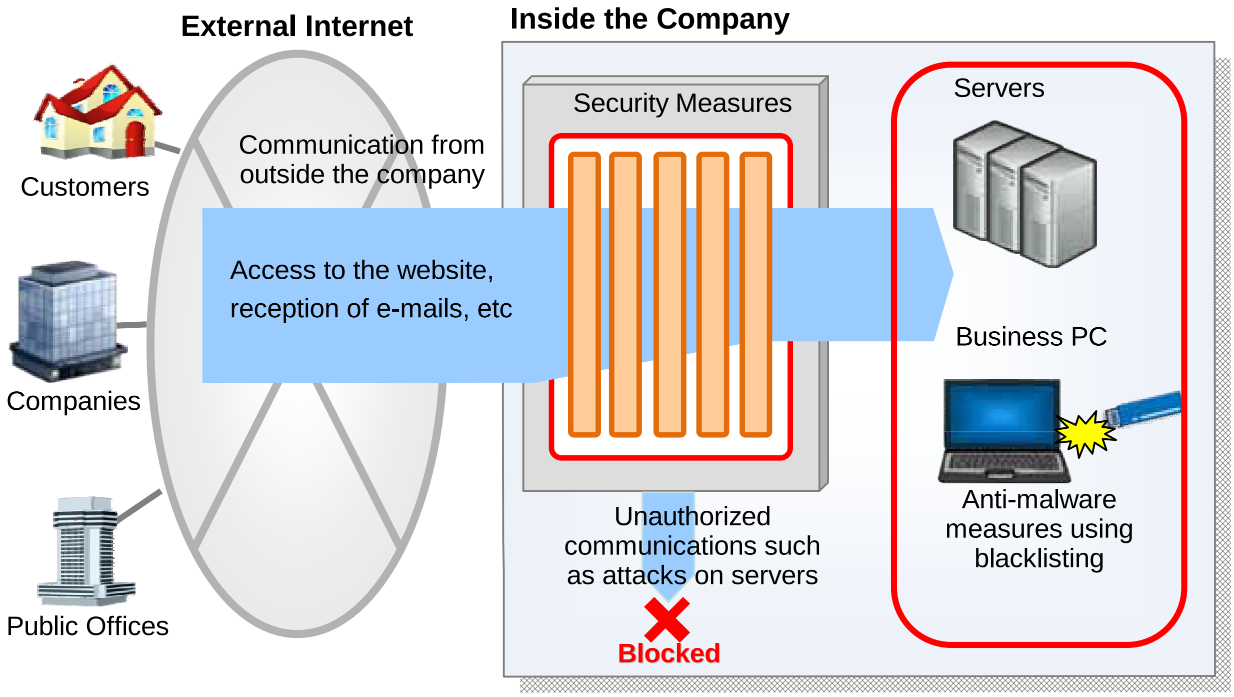
External Internet
Inside the Company
Customers
Companies
Public Offices
Communication from outside the company
Access to the website, reception of e-mails, etc
Security Measures
Unauthorized communications such as attacks on servers
Blocked
Servers
Business PC
Anti-malware measures using blacklisting

Fig. 1 Overview of Previous Security Measures

To address this need, we decided to introduce “anti-malware measures using whitelisting,” an approach that has begun to gain ground as an effective measure against zero-day attacks, into our business PCs with the aim of reinforcing security measures against new types of malware.

2. Introduction of Anti-malware Measures using Whitelisting

2.1 Overview of Anti-malware Measures using Whitelisting

Anti-malware measures using whitelisting represent a system that allows preregistration of normal program operations (i.e., whitelisting) and stops the operation of any non-registered operations if detected.

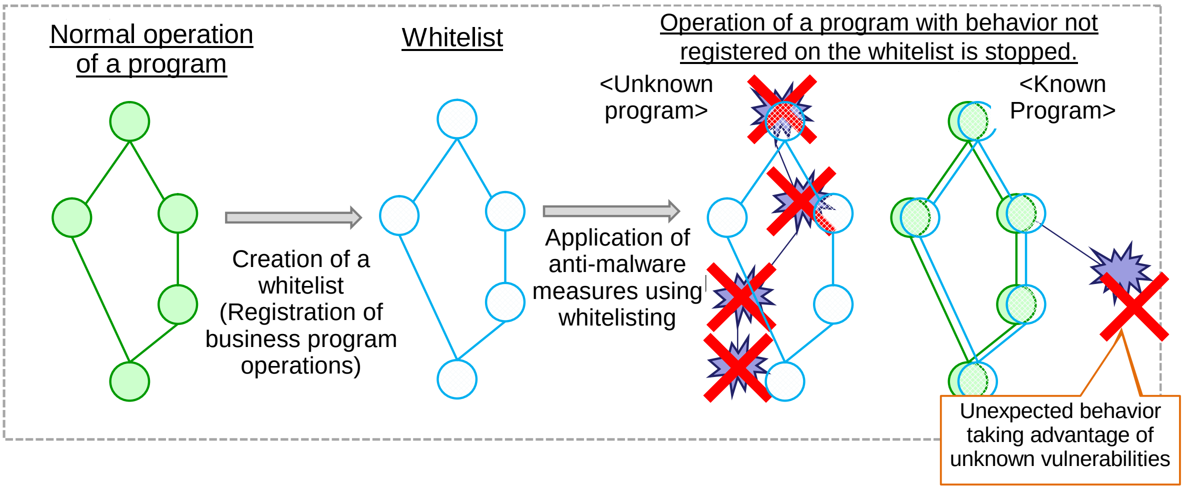
Normal operation of a program
Whitelist
Operation of a program with behavior not registered on the whitelist is stopped.
<Unknown program>
<Known Program>
Creation of a whitelist (Registration of business program operations)
Application of anti-malware measures using whitelisting
Unexpected behavior taking advantage of unknown vulnerabilities

Fig. 2 Overview of Anti-malware Measures using Whitelisting

The anti-malware measures using whitelisting presented in this paper mean software capable of operating in the following two modes in accordance with the operating status.

Detection mode: Setting in which the details and history of unauthorized behavior of programs not registered on the whitelist are acquired as detection logs

Block mode: Setting in which unauthorized behavior is blocked by interrupting such behavior if detected in addition to the detection mode operation

2.2 Pre-verification with the Goal of Introduction into the Kyushu Electric Power Company Environment and Issues that arose during Pre-verification

Kyushu Electric Power Company comprises various operating departments including sales, power generation, and power transmission and distribution, each of which has a large number of systems with various types of configurations such as centralized and distributed processing depending on the department.

In preparation for the introduction of anti-malware measures using whitelisting into our in-house business PCs, we performed pre-verification to verify detection performance and identify and sort operational issues.

Terminals verified: Information Systems Dept. (Approximately 100 units) and other operating depts. (Approximately 40 units in 11 depts.)
Terminal environment: Windows OS
Conventional anti-malware measures using blacklisting are also used.
Verification period: April to December 2012 (9 months)
Operation mode: Detection mode

During verification, the standard whitelist attached to the whitelist-based defense against malware was utilized, but so many program operations were listed in detection logs as to interfere with the operation of the systems.

To resolve this problem, it was necessary to carefully examine detection logs and make additional registrations on the whitelist.

2.3 Consideration of Resolution of Issues

Although deleting a large portion of the detection logs to enable practical operation presented a challenge, the results of examination of the history acquired in the detection mode confirmed the characteristics listed below.

(1)The program operations of standard OA applications such as Office and Adobe Reader were also detected.

(2)Operations of programs involving communication with business servers were detected.

(3)Operations such as Cookie information uploads to advertizing sites when browsing the Internet were detected.

(4)Free software operations were detected.

With exception of (1) to (4) above, approximately 280 operations (approximately 1% of the whole) were detected and, after careful scrutiny, it was expected that making additional registrations on the whitelist would resolve the problem.

The measures listed below were implemented to resolve the problem.

(1) Quality improvements to the software were urged to prevent the detection of programs and operations free of security problems.

(2) & (3) The scope of defense provided by the newly-introduced anti-malware measures using whitelisting was limited to “information theft.”
In concrete terms, modifications were made to ensure that communications completed in-house would not be detected.

(4) A software installation prevention function was mounted in tandem with PC replacements to make it impossible to install applications unrelated to business such as free software.

It was anticipated the above measures would result in deletion of a large portion of the detection logs.

2.4 Introduction to all In-house Business PCs

Based on the anticipated deletion of a large portion of the detection logs, the anti-malware software using whitelisting was installed in all in-house business PCs.

Target terminals: 13,600 units
Terminal environment: Windows OS
Conventional anti-malware measures using blacklisting are also used.
Installation period: November 2014 to March 2015
Operation mode: Detection mode

3. Future Developments and Closing Comments

3.1 Present State of Operation and Future Developments

To realize the intended goal of preventing damage such as information leakage caused by intrusion by new types of malware, migration to the block mode needs to be implemented as soon as possible. That being said, program operations for systems commenced after pre-verification and operations of programs used by specific offices have not yet been registered on the whitelist, presenting the risk of interference with business operations. To address this situation, adoption of the following two stages has been planned.

Step 1: Monitoring in the Detection Mode

Program operations that have not been whitelisted will be detected and reported to the system administrator to enable monitoring of intrusion by new types of malware.

In addition, detection logs will be carefully examined and operations that present no risk added to the whitelist to improve the accuracy of the whitelist.

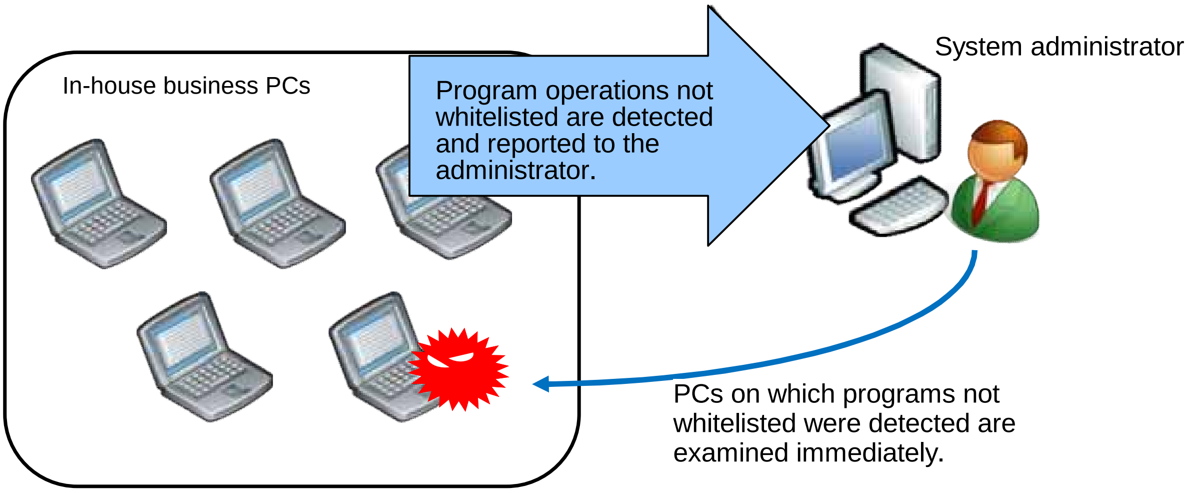
In-house business PCs
Program operations not whitelisted are detected and reported to the administrator.
System administrator
PCs on which programs not whitelisted were detected are examined immediately.

Fig. 3 Detection Mode Operation (Step 1)

[Effects of Monitoring in the Detection Mode]

Detecting program operations that have not been whitelisted will make it possible to detect new types of malware.

Moreover, careful examination of acquired individual detection logs will not only improve the accuracy of the whitelist, but also enable closer investigation of factors such as damage status and routes of infection in the event of intrusion by a new type of malware.

Step 2: Block Mode Operation

In addition to the detection mode operation, the block mode will block the operation of programs that have not been whitelisted as soon as they are detected.

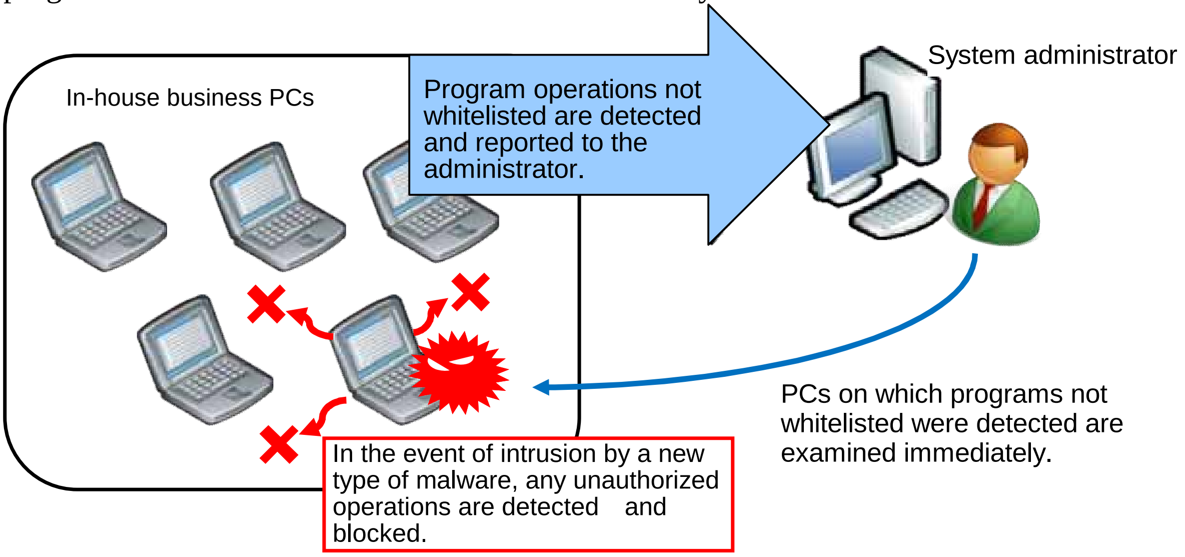
In-house business PCs
Program operations not whitelisted are detected and reported to the administrator.
System administrator
PCs on which programs not whitelisted were detected are examined immediately.
In the event of intrusion by a new type of malware, any unauthorized operations are detected and blocked.

Fig. 4 Block Mode Operation (Step 2)

[Effects of Block Mode Operation]

Even in the event of intrusion by a new type of malware, the block mode will make it possible to detect and block attempts by the malware to extract confidential information.

3.2 Outstanding Issues

Although additional registrations on the whitelist seem to be leading to a decrease in the number of incidents detected compared to the pre-verification stage, further improvements in the accuracy of the whitelist will need to be made for the application of the block mode in the future, necessitating the realization of greater efficiency in registration work.

3.3 Conclusion

Infection of in-house PCs by new types of malware in the past presented the risk of continued extraction of confidential information due to failure to notice the infection.

At the present time, although the introduction of anti-malware measures using whitelisting enables instantaneous detection of new types of malware even if in-house business PCs are infected with such malware, the early application of the block mode will be essential in the future.

On the other hand, constant changes in the system usage environment due to modifications, renewal and the introduction of new systems will make it necessary to further improve the efficiency of whitelisting.

In concrete terms, the accurate operation of anti-malware measures using whitelisting will need to be ensured by speeding up the process of identifying and considering security risks related to programs recorded in detection logs to determine whether or not they can be added to the whitelist.