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

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

http: //d2.cigre.org
/

2017 Colloquium
September 20 to 22, 2017
Moscow – RUSSIA

Preferential Subject N°- PS2

Introduction of AI-based Anti-malware Software to resist Cyber Threats

KAZUKI KITAHARA
KYUSHU ELECTRIC POWER CO., INC.
JAPAN
kazuki_kitahara@kyuden.co.jp

1. Introduction

Recent years have seen a dramatic increase in threats posed by diverse cyber attacks and this has led to incidents such as leakage of personal information, including pension information, due to malware infections and the rapidly-increasing number of ransomware attacks, making the continuation of business operations of targeted entities difficult. Serving countless customers and shouldering the responsibility for the important electricity infrastructure, the power industry needs to build an environment capable of resisting these threats.

2. Existing Approaches to handling Cyber Threats

The main approach currently used as a countermeasure against cyber threats is to check whether or not target files are infected with malware by matching them to malware information that has already been identified.

However, this approach presents the following problems:

- Inability to detect malware unless target files infected with malware match any of the already-identified malware information;
- The need to frequently update malware information used as a base for matching because malware information needs to be always up-to-date; and
- Inability to keep up with constantly increasing and changing malware because malware information cannot be created without malware samples and it takes time to create malware information, even if samples are available.

In addition, anti-malware approaches using whitelisting and blacklisting methods to put restrictions on communication and files have the following problems:

- Inability to flexibly handle non-regular operations that may be required, for example, due to the inability to perform processing that overrides restrictions, resulting in interference with business operations; and
- Frequent updating of lists, presenting operational issues.

3. Existing Approaches to handling Cyber Threats

To resolve the problems with the existing approaches, we have conducted studies on the introduction of AI-based anti-malware software.

AI-based anti-malware software extracts several millions of features from huge numbers of normal and abnormal files and uses AI (Artificial Intelligence)-based machine learning to learn features, thereby determining whether or not target files are suspicious by comparing their features with the features learned using machine learning. Therefore, we expect that this AI-based approach will enable resolution of the problems with the existing approaches for the reasons cited below.

- Ability to determine whether or not target files are infected with malware even if their features do not perfectly match already-identified malware features because this approach compares the features of target files with features learned from existing files using machine learning (Ability to handle unknown malware)
- Elimination of the need for frequent updating because machine learning uses features identified from existing files

4. Conclusion

This paper has presented the results of our study into the effectiveness of AI-based anti-malware software with the aim of building an environment capable of handling different types of cyber threats.

The implementation of full liberalization of the electricity retail market means that our company has become one of many now available for selection as an electricity supplier by customers, and this in turn means that we need to make even greater efforts to gain and maintain the trust of our customers. To this end, we will make continued efforts to deal with constantly changing cyber threats.