JPCERT-PR-2017-02
Issued: 2017-4-13

JPCERT/CC Activities Overview [January 1, 2017 - March 31, 2017]

Activity Overview Topics

- Topic 1 - JPCERT/CC releases a practical guide focused on Active Directory security

Active Directory (AD) is often targeted in advanced cyber attacks. In light of this situation, JPCERT/CC released "Using Logs to Detect Attacks Against Active Directory and Countermeasures" (Japanese only), a document dealing specifically with AD security, on March 14, 2017.

Numerous cases of advanced cyber attacks including targeted attacks have occurred in Japan as well, presenting a serious security threat. JPCERT/CC has confirmed many cases where a security breach in AD led to an abuse of AD's domain administrator account, spreading infection to other servers and computers. Moreover, after analyzing reported incidents, JPCERT/CC found that in some cases a delayed response to AD's vulnerabilities allowed the security breach to occur, while in other cases logs were not saved properly, making it difficult to investigate the damage status. These cases point to the need for improvement of AD log checks and AD operation at many organizations, in order to protect AD from attacks or localize the damage of advanced cyber attacks by quickly detecting any breach of defense and conducting an investigation.

This document is based on the knowledge obtained by JPCERT/CC through the support it has provided in responding to many advanced cyber attacks. It is a practical guide that contains information about typical attack methods used against AD as well as how to detect and take measures against these attacks. Moreover, the document is structured so that readers can easily find the information they need, making it a useful reference even in an emergency situation when there is no time to read it through, and for those engaged in system operation and incident handling.

Using Logs to Detect Attacks Against Active Directory and Countermeasures (Japanese only)
https://www.jpcert.or.jp/research/AD.html

- Topic 2 - JPCERT/CC releases a tool to visualize the results of malware clustering based on similarity

On March 10, 2017, JPCERT/CC released "impfuzzy for Neo4j," a tool that clusters malware based on similarity and visualizes the results.

In recent years, a large amount of malware is created by being partially modified. As a result, identifying the extent of modification and extracting the malware to be analyzed as well as new types of malware have become important tasks in malware analysis.
The new impfuzzy for Neo4j is a tool developed with the aim of supporting activities related to malware analysis. It is expected that the tool will be widely used by organizations for malware analysis related to incident handling, investigations and research related to malware analysis, and other applications.

impfuzzy for Neo4j calculates the similarity of malware using a method called impfuzzy and generates a graph (network) based on the results. Then, the graph is clustered using a method called network analysis, and the results are visualized. Visualization is performed using Neo4j, which is a graph database.

impfuzzy, which is used to calculate the similarity of malware, is a unique method proposed by JPCERT/CC for calculating the hash value of an execution file, and it calculates a value called fuzzy hash based on the Import API of an execution file. Compared with conventional methods, impfuzzy is more suited to the classification of executable file type malware.

As for other tools implementing impfuzzy, JPCERT/CC already provides "pyimpfuzzy," which is a python module for calculating and comparing impfuzzy, and "impfuzzy for volatility," which enables investigation of similar files from a memory image using impfuzzy. With the addition of impfuzzy for Neo4j, the available tools now enable impfuzzy to be used for each of the malware analysis operations, from the calculation of malware hash value to comparison and visualization of similarity.

The impfuzzy-related tools including the new impfuzzy for Neo4j are made available on GitHub, a web service for sharing software development projects.

Malware Clustering Using impfuzzy and Network Analysis ~impfuzzy for Neo4j~ (2017-03-23)
http://blog.jpcert.or.jp/2017/03/malware-clustering-using-impfuzzy-and-network-analysis---impfuzzy-for-neo4j-.html

JPCERTCC/aa-tools GitHub - impfuzzy
https://github.com/JPCERTCC/aa-tools/tree/master/impfuzzy/

-Topic 3 - ICS Security Conference 2017 is held

On February 21, JPCERT/CC held the Industrial Control System (ICS) Security Conference 2017 in Tokyo. This year's theme was "Preparing for Future Incidents."

About 270 visitors attended the conference, representing a diverse mix of professionals: 32% asset owners, 25% ICS equipment vendors, 16% system vendors, 11% engineering firms, and 7% researchers. Compared to the first conference held eight years ago, when the event attracted only the limited interest of ICS vendors, participants have nearly quadrupled, with much of the growth accounted for by asset owners. This rise in interest seems to indicate a power trend within the industry toward stronger ICS security.

This year's program also included presentations selected through an open application process. While this was the first time ever to solicit speakers in this manner, people in various positions submitted presentation proposals.

ICS Security Conference 2017 (Program) (Japanese only)
https://www.jpcert.or.jp/event/ics-conference2017.html

ICS Security Conference 2017 (Lecture Materials) (Japanese only)
https://www.jpcert.or.jp/present/#year2017