JPCERT/CC®

JPCERT-PR-2015-05
Issued: 2016-01-14

JPCERT/CC Activities Overview [October 1, 2015 - December 31, 2015]

Activity Overview Topics

－Topic 1－ JPCERT/CC releases documents to aid measures against advanced cyber attacks

To help promote efforts to implement effective measures against advanced cyber attacks, JPCERT/CC released a document titled "How to Use and Analyze Logs in Dealing with Advanced Cyber Attacks" (in Japanese) on November 17, 2015, and partially reviewed and updated the "CSIRT Materials (Concept, Establishment, and Operation)" (in Japanese) available on its website.
Numerous cases of advanced cyber attacks have emerged in Japan as well, presenting a new security threat to many organizations. Unlike conventional attacks, advanced cyber attacks cannot be fully prevented through detection and protective measures alone. Therefore, the success of any countermeasure hinges on the ability to identify and deal with abnormalities as early as possible, based on the assumption that an attack and intrusion can occur any time without being noticed.

By properly configuring the logging function of existing equipment and checking captured log data at the right timing, it is possible to detect abnormalities relatively quickly and with no need for any major additional investment. However, due to the absence of a document that outlines how to do this, there have been many cases in which the logging function has not been sufficiently utilized.

"How to Use and Analyze Logs in Dealing with Advanced Cyber Attacks" was released with the aim of helping to improve this situation, and from the perspective of preparing for and effectively dealing with advanced cyber attacks. This document describes the approach for leaving traces of the attacker's activities as log data on commonly used equipment, as well as the method used to identify those traces in logs.

"CSIRT Materials (Concept, Establishment, and Operation)" have served as a definitive guide for establishing an internal CSIRT ever since they were released in 2008. Advanced cyber attack incidents are not an issue that can be addressed only through the local and isolated efforts of system administrators. In some cases, concerted efforts with partners and other organizations are required, and this highlights the key importance of the role played by an internal CSIRT backed by the active involvement of the management.

To reflect such changes in the operational context, JPCERT/CC has released updated versions of the "CSIRT Materials" for the concept, establishment, and operation phases.

The latest update contains a description of the threat of advanced cyber attacks (Advanced Persistent Threats) and offers advanced tactics for countering such attacks. Existing materials have also been supplemented with new information on implementing risk assessments across the organization, defining the level of tolerance for risk, information sharing and coordination among CSIRTs, the roles to be played by CSIRT, skills required of CSIRT personnel, and so on.

－Topic 2－ JPCERT/CC releases detection tools and analysis scripts for malware used in targeted attacks

On October 28, 2015, JPCERT/CC Analysis Center released tools for analyzing malware used in targeted attacks.

JPCERT/CC engages in activities designed to help respond to targeted attack incidents based on incident reports, etc., and also conducts technical investigations and malware analysis related to targeted attacks. The newly released tools were also created in relation to these activities and are intended to broadly support incident response and investigations.

Two tools were released: "apt17scan.py" and "emdivi_string_decryptor.py." Both can be used to analyze malware used by groups of attackers targeting Japanese organizations.

"apt17scan.py" is a tool for scanning memory images to detect a number of malware used by specific group of attackers, and extracting the configuration information of any detected malware. It is implemented as a plugin for The Volatility Framework, which is a memory forensics tool.
On the other hand, "emdivi_string_decryptor.py" is a tool for decoding encoded strings contained in remote control malware called Emdivi. It is implemented as an IDAPython script for the IDA disassembler.

These tools were also introduced in JPCERT/CC's presentation "Revealing the Attack Operations Targeting Japan" at CODE BLUE 2015, held on October 28, 2015. JPCERT/CC English Blog articles introducing these tools were also released along with the tools.

The tools are made available on GitHub, a shared web service for software development projects.

JPCERTCC/aa-tools・GitHub
https://github.com/JPCERTCC/aa-tools

A Volatility Plugin Created for Detecting Malware Used in Targeted Attacks
http://blog.jpcert.or.jp/2015/11/a-volatility-plugin-created-for-detecting-malware-used-in-targeted-attacks.html
Decrypting Strings in Emdivi

－Topic 3－ Vulnerability scores based on Common Vulnerability Scoring System (CVSS) v3 now available on JVN

JPCERT/CC started announcing vulnerability scoring results based on CVSS v3 on JVN from December 1, 2015.

Vulnerabilities that are built into software products can have their severity levels indicated by assessing a number of factors in a comprehensive manner, including their cause, type, reproducibility, and whether an attacker can exploit them remotely.
CVSS is a system commonly used today to indicate the severity of vulnerabilities.

FIRST, the group that operates CVSS, updated the current CVSS v2 and officially released v3 in June 2015. In response, JPCERT/CC started listing scores for both CVSS v2 and v3 in its vulnerability advisories released on JVN from December 1.

With CVSS v3, it is now possible to make an impact assessment that focuses on the components where vulnerabilities exist, instead of assessing the entire system. It also enables the assessment of vulnerabilities in terms of their difficulty of being exploited, based on more detailed criteria. As such, it is highly anticipated as a tool for obtaining vulnerability scores that reflect the actual threat more accurately.

JPCERT/CC will lead the way in starting the application of CVSS v3 and promote its adoption by Japanese organizations.