JPCERT-PR-2018-01
Issued: 2018-1-16

JPCERT/CC Activities Overview [October 1, 2017 – December 31, 2017]

Activity Overview Topics

- Topic 1 - Document and tool for investigating traces of attack activities now available

Investigation of incidents including cyber attacks that infiltrate various information systems of an organization normally has to cover a lot of ground, which makes it a huge challenge to conduct the investigation rapidly without overlooking important leads. For this reason, organizations require the means and support tools to grasp the full extent of the damage as accurately as possible, and to collect information needed to formulate a remedy.

To address such needs, JPCERT/CC has released the second version of the report "Detecting Lateral Movement through Tracking Event Logs," which intends to help investigations into traces that attack activities leave behind in devices within an organization. Along with this document, JPCERT/CC has also released LogonTracer, a tool for visualizing event logs. These are intended to help with a wide range of activities required in incident response and investigations of recent years.

"Detecting Lateral Movement through Tracking Event Logs" summarizes the findings of an investigation conducted to find out what kinds of logs are generated when common attack tools are executed, and what settings will ensure the logs will contain sufficient information. The new version is a major update on the first version released in June 2017 presenting new findings on an investigation that covered a different and broader set of tools. It also contains information about updates in the operating systems used to investigate traces, and the format of the report has been changed. These updates and improvements have resulted in a report that is easier to use as a guide when conducting investigations into traces left behind by the latest attacks.

As for the investigation of traces described in the report, a lecture entitled "Pursue the Attackers – Identify and Investigate Lateral Movement Based on Behavior Pattern –" was given at CODE BLUE 2017 on November 9, 2017, and a lecture entitled "Hunting Attacker Activities - Methods for Discovering and Detecting Lateral Movements" was given at Botconf 2017 on December 8, 2017. When the report was released, details of the report were also provided in JPCERT/CC's English blog.

LogonTracer, the event log visualization tool, can associate host names (or IP addresses) with account names and visualize (chart) the result. It facilitates the analysis of event logs, an essential part of incident

investigation, by visualizing the process, which has been well-received by many users.

At “Incident Response Hands-On 2017,” a workshop held at Internet Week 2017 on November 29, 2017, JPCERT/CC staff conducted training by actually using the tool. When the tool was released, an article introducing the tool was posted on JPCERT/CC’s English blog.

The tool can be obtained on GitHub, a shared web service for software development projects, and a Docker image, which has the environment for running the tool already setup, is made available on Docker Hub.

■Documents related to “Detecting Lateral Movement through Tracking Event Logs”

Detecting Lateral Movement through Tracking Event Logs
https://www.jpcert.or.jp/english/pub/sr/ir_research.html

Research Report Released: Detecting Lateral Movement through Tracking Event Logs (Version 2)
http://blog.jpcert.or.jp/2017/12/research-report-released-detecting-lateral-movement-through-tracking-event-logs-version-2.html

■Documents related to LogonTracer

JPCERTCC/LogonTracer - GitHub
https://github.com/JPCERTCC/LogonTracer

jpcertcc/docker-logontracer - DockerHub
https://hub.docker.com/r/jpcertcc/docker-logontracer/

Visualise Event Logs to Identify Compromised Accounts - LogonTracer - (November 30, 2017)
http://blog.jpcert.or.jp/2017/11/visualise-event-logs-to-identify-compromised-accounts---logontracer-.html

- Topic 2 - Special web page published on ransomware countermeasures

Ransomware is a type of malware that places a certain restriction on the infected computer and demands payment of a ransom in exchange for removing the restriction. The very first ransomware dates back to 1989, but it was around 2012 when many varieties of ransomware started showing up. From around 2015, against a backdrop of the growing popularity of virtual currency, ransomware-related damage started reaching serious proportions at corporations. Then in 2016, the number of reported damage in Japan reached record levels in 2016. In 2017, self-propagating ransomware like WannaCrypt and NotPetya wreaked havoc and the damage they caused was widely covered by the media. Today, ransomware is said to be one of the most serious cyber threats.

In light of these circumstances, JPCERT/CC published a special web page on how to protect against ransomware on October 26, 2017. This web page provides a wealth of relevant information with the aim of raising awareness among users. The web page introduces major ransomware that JPCERT/CC has identified in Japan and explains how to reduce and prevent damage caused by ransomware, as well as what to do in the case of an infection.

JPCERT/CC is also a Supporting Partner of the “No More Ransom” project, an international effort to eliminate ransomware, and is working with related organizations around the world to develop effective countermeasures. The web page also provides information about JPCERT/CC’s policies for its activities both at home and abroad.

Special web page on ransomware countermeasures (Japanese)
https://www.jpcert.or.jp/magazine/security/nomore-ransom.html