JPCERT CC®

JPCERT/CC Activities Overview

July 1, 2019 ～ September 30 , 2019

JPCERT Coordination Center

October 17, 2019

JPCERT CC®

Activity Overview Topics

－Topic 1－ "MalConfScan," a tool for extracting malware configuration information, and a plugin called "MalConfScan with Cuckoo" released

To deal with the daily barrage of new malware variants, malware analysis is becoming increasingly automated. Many of the automated analysis systems developed to date have focused mainly on understanding the behavior of programs on Windows such as communication and the creation of file and registries. Malware analysts, however, spend far more time on extracting configuration information hard-coded in malware than on understanding such malware behavior, and are calling for increased work efficiency in this area.

To address such needs, JPCERT/CC released "MalConfScan," a tool for extracting malware configuration information from a memory image, and a plugin called "MalConfScan with Cuckoo," designed to be used for malware analysis, incident handling and investigations, and various other activities. They are freely available on GitHub.

This tool will significantly reduce the amount of time spent on malware analysis and incident handling. It currently handles 25 types of malware, with more to be added going forward through regular updates.

As for "MalConfScan with Cuckoo," JPCERT/CC gave a presentation entitled "MalConfScan with Cuckoo: Automatic Malware Configuration Data Extraction and Memory Forensic" at Black Hat USA 2019 held on August 8, 2019, and introduced the tool on JPCERT/CC Eyes.

■References related to MalConfScan with Cuckoo

JPCERTCC/MalConfScan-with-Cuckoo – GitHub
https://github.com/JPCERTCC/MalConfScan-with-Cuckoo

JPCERT/CC Eyes: MalConfScan with Cuckoo: Plugin to Automatically Extract Malware Configuration
https://blogs.jpcert.or.jp/en/2019/08/malconfscan-with-cuckoo.html

■References related to MalConfScan

JPCERTCC/MalConfScan – GitHub
https://github.com/JPCERTCC/MalConfScan

JPCERT/CC Eyes: Extract Malware Configuration with MalConfScan
https://blogs.jpcert.or.jp/en/2019/08/malconfscan.html

ー Topic 2ー　Suguru Yamaguchi, First Board Chairman of JPCERT/CC, inducted into the Internet Hall of Fame

On September 27, 2019, it was announced that Dr. Suguru Yamaguchi, a founding member of the JPCERT/CC and its first Board Chairman, had been inducted into the Internet Hall of Fame.

The Internet Hall of Fame is a program whose objective is to recognize individuals who have made extraordinary contributions to the development of the Internet. Launched in 2012 by the Internet Society (ISOC)(*1), a non-profit organization, it has inducted 103 individuals, including 5 Japanese, to date. This year, 11 inductees, including Dr. Yamaguchi, were given the honor.

Dr. Yamaguchi's induction is in recognition of his dedication to research and capacity building on cyber security, contributions to FIRST, an organization in which CSIRTs around the world participate, efforts to enhance collaboration among CSIRTs in Africa and Asia, and leadership in the WIDE Project(*2) and AI3(*3). Dr. Yamaguchi passed away in May 2016.

Dr. Suguru Yamaguchi, first board chairman of JPCERT/CC and Internet Hall of Famer

New Class of Internet Hall of Fame Inductees Announced (ISOC)
2019 inductees recognized for contributions to Internet growth, access, and security around the world
https://www.internetsociety.org/news/press-releases/2019/new-class-of-internet-hall-of-fame-inductees-announced/

INDUCTEES　Suguru Yamaguchi (ISOC)
https://internethalloffame.org/inductees/suguru-yamaguchi

Dr. Suguru Yamaguchi, the First Board Chairman of JPCERT/CC, Entered the Internet Hall of Fame as an Inductee
https://www.jpcert.or.jp/english/pub/2019/PR20190930_Internet_Hall_of_Fame.html

*1 Internet Society (ISOC): https://www.internetsociety.org/about-internet-society/
The Internet Society (ISOC) was founded in 1992 by a number of people involved with the Internet Engineering Task Force (IETF). From those early days, one of our principal rationales is to provide an organizational home for and financial support for the Internet standards process.

*2 WIDE Project: http://www.wide.ad.jp/
WIDE Project is a joint research project between industry and universities on wide distributed computing environment. The project was launched by Jun Murai and other contributors in 1988 to "discuss the challenges in constructing a distributed computing system for people and the society by connecting computers and other devices on the earth" Over 100 organizations in Japan from universities to research institutions to private companies participate in the project.

*3 AI3: https://www.kri.sfc.keio.ac.jp/ORF/2000/press/ai3.pdf

ー Topic 3ー　JPCERT/CC 2019 letter of thanks presented to persons who made significant contributions to cyber security activities

With the aim of minimizing damage caused by cyber security incidents taking place in Japan (herein, "incidents"), JPCERT/CC undertakes support activities to help respond to incidents, provision of early warning information to help prevent incidents, analysis of malware, coordination related to the handling of vulnerabilities in software products, and other relevant activities. To ensure these activities are conducted smoothly and effectively, various forms of assistance are essential. At JPCERT/CC, we have established a system for presenting letters of thanks as a sign of our deep appreciation to those individuals who have made particularly significant contributions with respect to cyber security activities.

This year, we presented a letter of thanks and a commemorative shield to SAKURA internet Inc. in recognition of its contributions to and cooperation in promoting security measures by domestic cloud

service operators, and increasing the level of security measures across the industry. The other recipient this year was Kazushi Otani of Sumitomo Chemical Co., Ltd., who endeavored to raise security awareness within the petrochemical industry as the leader of the Information Security Working Group of the Japan Petrochemical Industry Association's Information Communication Committee, and who also assisted JPCERT/CC's activity to ensure ICS security.

Letter of thanks presented to persons who made significant contributions to cyber security activities (Japanese)
https://www.jpcert.or.jp/press/priz/2019/PR20190808-priz.html