JPCERT/CC®

JPCERT-PR-2018-04
Issued: 2018-10-16

JPCERT/CC Activities Overview [July 1, 2018 – September 30,2018】

Activity Overview Topics

– Topic 1– "Fact-finding Survey Report on Ransomware Threats and Damages" released

On July 30, JPCERT/CC released "Fact-finding Survey Report on Ransomware Threats and Damages," which provides a broad picture of the situation with regard to ransomware mainly in Japan.

Infection and attack methods of ransomware continue to change each year. Most of the early types of ransomware relied on some kind of action on the part of users, such as opening an e-mail or accessing a compromised website, to cause an infection. Since 2017, however, self-propagating malware like WannaCrypt (WannaCry) started to appear, causing a pandemic in which a large number of computers get infected around the world in a short period of time. There are also types of ransomware that destroy the infected system while pretending to demand a ransom, and those whose true aim seems to be to disrupt investigations into traces of targeted attacks.

In fiscal year 2017, JPCERT/CC conducted a questionnaire survey to find out the actual situation of ransomware damages suffered by Japanese companies. This survey revealed that 35% of the organizations had an experience of ransomware infection, and 16% were unable to restore data encrypted by ransomware. This report summarizes these and other survey results and relevant analyses, as well as other useful information such as the infection routes of ransomware, background to the growth of infection risks in Japan, and development of threats.

Fact-finding Survey Report on Ransomware Threats and Damages [Japanese]
https://www.jpcert.or.jp/research/Ransom-survey.html

– Topic 2– Japanese version of the "FIRST PSIRT Services Framework 1.0 Draft" released

In cooperation with Software ISAC, an organization established within the Computer Software Association of Japan (CSAJ), JPCERT/CC created the Japanese version of the "PSIRT Services Framework Version 1.0 Draft," a document published by the Forum of Incident Response and Security Teams (FIRST) for product developers, and released it on FIRST's website.

PSIRT stands for Product Security Incident Response Team and represents a function for responding

internally within organizations to risks attributable to vulnerabilities in products provided by the organizations. The "PSIRT Services Framework" gives an overview of PSIRT and its concepts, and describes its organizational model, functions and services, referring to the activities of various PSIRTs that join FIRST. The document serves as a useful guide for companies planning to launch a PSIRT or review current activities since it helps them pinpoint the functions they need and consider the optimal organizational structure.

While increasing numbers of companies in Japan are establishing and operating a PSIRT, many product developers have yet to develop a concrete system even though they understand the importance of a PSIRT function. It is hoped that the Japanese version of the document will be utilized by many such product developers.

Incidentally, the "Version 1.0 Draft" has been updated and released as "PSIRT Services Framework Version 1.0" on FIRST's website, and work is underway to update the Japanese version as well. JPCERT/CC also plans to work with CSAJ and Software ISAC to pursue educational activities for product developers.

Abridged Japanese translation of the PSIRT Services Framework Version 1.0 Draft [Japanese]
https://first.org/education/FIRST_PSIRT_Services_Framework_v1.0_draft_ja.pdf

JPCERT/CC Studies/Research [Japanese]
"Abridged Japanese translation of the FIRST PSIRT Services Framework Version 1.0 Draft"
https://www.jpcert.or.jp/research/psirtSF.html

Computer Software Association of Japan (CSAJ) [Japanese]
Japanese translation of the "PSIRT Services Framework 1.0 Draft" released
http://www.csaj.jp/NEWS/pr/180719_psirt.html

Cybozu Inside Out | Cybozu Engineers' Blog [Japanese]
Introducing the PSIRT Framework
https://blog.cybozu.io/entry/2018/07/18/080000

― Topic 3― "Security for Introducing Industrial IoT in Factories: The First Step" released

On August 9, JPCERT/CC released "Security for Introducing Industrial IoT in Factories: The First Step," a reference document describing basic security countermeasures to be taken when introducing industrial IoT to Industrial Control Systems (ICS) in factories.

In recent years, use of IoT is spreading in the industrial sector as well, in the hope that it will help boost productivity and make up for the shortage of labor. However, there are many cases in which IoT is introduced without giving full consideration to security risks involved or taking sufficient countermeasures, and administrators on the front line have been asking for a practical security guide related to IoT.

This document is a guide that illustrates the importance and idea of security in introducing industrial IoT and describes security countermeasures to be taken in each process (from the formulation of specifications at the time of introduction to actual operation) from the perspective of management, as well as technical security countermeasures that should be taken for each component of the IoT network on site (IoT devices, networks inside the factory, servers, external networks and the cloud). The document is designed to make it easy to find the necessary information, for instance, by including a "Countermeasure Navigation Map," an IoT network configuration diagram that gives the page numbers where information about relevant countermeasures can be found for each component. It also explains the basics of security countermeasures assuming readers include business managers and front-line staff (managers and technical staff) of small and midsize manufacturers, which often do not have security specialists.

See 3.5 "Security for Introducing Industrial IoT in Factories: The First Step" released for details.

Security for Introducing Industrial IoT in Factories: The First Step [Japanese]
https://www.jpcert.or.jp/ics/information06.html

－ Topic 4－ 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 Katsuya Uchida, Koji Nonoshita and Yasuharu Shimada in July 2018. Mr. Uchida and Mr. Nonoshita have contributed to the reduction of phishing damages throughout Japan over many years in their capacities as chair and deputy chair of a working group for the Council of Anti-Phishing Japan. Mr. Shimada has contributed to raising the overall level of handling vulnerabilities throughout the industry in Japan through his work for I-O Data Device, Inc., working hard to improve the security of the company's products, and actively announcing vulnerabilities detected by the company to inform general users on Japan

Letter of thanks presented to persons who made significant contributions to cyber security activities [Japanese]
https://www.jpcert.or.jp/press/priz/2018/PR20180710-priz.html