JPCERT/CC Activities Overview

January 1, 2020 ～ March 31, 2020

JPCERT Coordination Center
April 14, 2020

Activity Overview Topics

— Topic 1 — Business E-mail Compromise Survey Report released

On March 25, JPCERT/CC released the Business E-mail Compromise Survey Report, which summarized the results of a survey it conducted to investigate the actual situation of Business E-mail Compromise (BEC) in Japan with the cooperation of Japan Foreign Trade Council ISAC, the Japan Petrochemical Industry Association, and other organizations. The English version of the report was later published on 11 June.

BEC has become widely known since the Federal Bureau of Investigation (FBI) released related information in 2015. According to the FBI's Internet Crime Complaint Center (IC3), the number of victims was 166,349 with losses amounting to approximately 26.2 billion US dollars from June 2016 to July 2019. The threat of BEC is rising in Japan as well. A major case of BEC scam was widely publicized at the end of 2017, and in 2018 the first case of a BEC attack carried out using e-mails in Japanese was identified.

In light of these circumstances, JPCERT/CC conducted a questionnaire survey to collect detailed information about actual cases and interviews to investigate the status of measures against BEC, hoping to help prevent losses from BEC by clarifying the actual situation faced by Japanese organizations and disseminating the findings.

This report categorizes collected cases of BEC scams into five types and analyzes them. It explains three lesser-known characteristics of BEC: 1) a complex structure involving third parties, 2) exploitation of internal information stolen through other security incidents, and 3) exploitation of internal information stolen from other organizations.

In light of the survey results, the report also discusses measures against BEC in terms of preventive measures (countermeasures) and reactive measures (responses). JPCERT/CC hopes that the report will help many organizations to prevent losses from BEC.

■Business E-mail Compromise Survey Report
https://www.jpcert.or.jp/english/pub/sr/BEC-survey.html

— Topic 2 — EmoCheck, an Emotet malware detection tool, released

In January 2020, JPCERT/CC continued to receive numerous inquiries regarding the Emotet malware, which rapidly spread infections from late October 2019. Emotet steals e-mail conversations and addresses from infected hosts, hijacks e-mail conversation threads, and sends malicious e-mails to persons related to the infected organization. Organizations infected with Emotet often become aware of the infection through reports from related parties who received a malicious e-mail. Many organizations that consulted

with JPCERT/CC became concerned about a possible Emotet infection after being notified of the possibility by an external party, and they wanted to know how to find out if they were infected. Many of these consultations came from small and medium-sized enterprises, some of which did not have security measures in place, such as installing anti-virus software on client computers.

In light of these circumstances, JPCERT/CC developed EmoCheck, an Emotet detection tool, and released it on February 3. If a computer is infected with Emotet, this tool will locate the malware so that it can be removed. For information on how to use EmoCheck, see "1. Check Emotet infection with EmoCheck" on JPCERT/CC Eyes: "How to Respond to Emotet Infection (FAQ)."

Soon after the tool was released, a new version of the Emotet malware updated to evade detection by EmoCheck was found on the Internet. The latest version of EmoCheck released on February 10 has been enhanced to detect the new version of the malware as well. It is assumed that Emotet will undergo further updates to evade detection. JPCERT/CC will continue to respond by enhancing the tool.

■Github: JPCERT/CC / EmoCheck
https://github.com/JPCERTCC/EmoCheck/releases

■JPCERT/CC Eyes: How to Respond to Emotet Infection (FAQ)
https://blogs.jpcert.or.jp/en/2019/12/emotetfaq.html

—Topic 3— Japan Security Analyst Conference 2020 held Japan Security Analyst Conference 2020 held

The Japan Security Analyst Conference 2020 (JSAC2020) was held on January 17, 2020 at the Ochanomizu sola city Conference Center.
This conference was held with the aim of sharing information about ever-changing attack methods and new analytical techniques, to help improve the technical capabilities of security analysts who analyze and handle incidents.
Three hundred and one security analysts participated in this third conference. In response to the call for papers, 22 applications were submitted (exceeding last year's submissions numbering 18), of which 8 were chosen to be presented at the conference. The presentations covered technologies for incident analysis and response, including malware analysis, digital forensics, and incident handling, and provided the presenters' own new technological insights as well as information about analysis tools. Many questions were asked during the presentation, and experts actively exchanged opinions.

Presentation materials from JSAC2020 are made available excluding some speeches, and snapshots of the presentations are provided on JPCERT/CC Eyes as well. JPCERT/CC will continue to provide information and engage in activities that are useful to experts who analyze and handle incidents.

■Japan Security Analyst Conference 2020
https://jsac.jpcert.or.jp/en/index.html

■JPCERT/CC Eyes: Japan Security Analyst Conference 2020 -Part 1-
https://blogs.jpcert.or.jp/en/2020/02/japan-security-analyst-conference-2020-1.html

■JPCERT/CC Eyes: Japan Security Analyst Conference 2020-Part 2-
https://blogs.jpcert.or.jp/en/2020/02/japan-security-analyst-conference-2020-2.html

—Topic 4— ICS Security Conference 2020 held

On February 14, 2020, JPCERT/CC held the ICS Security Conference 2020 in Asakusabashi, Tokyo. About 300 visitors who registered in advance attended the conference, representing a diverse mix of professionals: 38.6% asset owners, 12.2% ICS equipment vendors, 7.1% ICS vendors, 9.1% ICS engineering firms and 8.3% researchers. When the first conference was held about 10 years ago, ICS vendors accounted for most of the participants. In recent years, however, asset owners have come to occupy a significant portion of the participants. This indicates that the importance of recognizing cyber security risks, collecting information needed to continue the company's business safely and taking action accordingly has become widely understood among ICS users as well.

At the conference, speeches were given on 7 topics, including 1 that was submitted in response to the call for papers. The presentations discussed cyber security policies in industrial fields, the latest threat information and scenarios to be anticipated regarding ICS security, standardization trends in ICS security, self-assessment of the maturity of ICS security management, and case examples of security measures taken by ICS user companies.

■JPCERT/CC Eyes: ICS Security Conference 2020 Report -Part1-
https://blogs.jpcert.or.jp/en/2020/03/ics-security-conference-2020-report--part1.html

■JPCERT/CC Eyes: ICS Security Conference 2020 Report -Part2-
https://blogs.jpcert.or.jp/en/2020/03/ics-security-conference-2020-report--part2.html