JPCERT/CC®

Japan Computer Emergency
Response Team Coordination
Center

JPCERT-PR-2017-03
Issued: 2017-7-13

JPCERT/CC Activities Overview [April 1, 2017 – June 30, 2017]

Activity Overview Topics

- Topic 1 - Ransomware WannaCrypt

Starting from May 12, 2017, numerous cases of infections with ransomware called WannaCrypt (also known as WannaCry) were reported around the world, severely impacting various aspects of society including public services provided by medical institutions and others in the United Kingdom, Europe and the rest of the globe. There were reports of damages from infection in Japan as well, with the victims ranging from leading manufacturers and local governments to individuals. JPCERT/CC analyzed information provided by overseas security organizations and confirmed that, as of the morning of May 13, approximately 2,000 computers were infected in Japan.

According to reports, servers and devices in 150 countries became infected. One of the reasons WannaCrypt was able to infect so many devices in such a short period of time is that, unlike other previous ransomware, it acted like a worm and was capable of infecting other computers by randomly sending out attack packets to any network.

On Friday, May 12 (local time), when reports of damages started coming in overseas, it was midnight and weekend in Japan. However, in order to be ready when affected organizations, etc., started inquiring about the situation on Monday, May 15, JPCERT/CC started sharing information with specialized institutions in other countries from Saturday, May 13, and issued an urgent alert on Sunday, May 14. JPCERT/CC started addressing requests for consultation from affected organizations, etc., from May 15, and based on analysis results of provided artifacts, updated the alert on May 17 and provided information about infection routes and countermeasures.

It is presumed that there are still many active servers around the world running OSs that have not been properly updated and containing vulnerabilities that allowed the infection to become widespread. JPCERT/CC is alerting the public against WannaCrypt and other cyber attacks that similarly exploit vulnerabilities in SMBv1.

Alert regarding PCs and servers that may be attacked via the Internet
https://www.jpcert.or.jp/english/at/2017/at170023.html

- Topic 2 - Incident Response Reports now available

Incident Response Reports (Japanese only), which introduce various incident cases and trends that JPCERT/CC handles, have now been launched.

JPCERT/CC has provided incident response services since its foundation. These services include receiving reports of computer security incidents related to Japan both from within and outside the country, providing support to affected organizations and communicating with related organizations to help prevent the spread of damages, and preventing the occurrence of similar incidents by sharing appropriate information.

Incident Response Reports will be written by members who work at the frontline of incident response and cover topics such as the latest incident cases and trends and investigation methods. JPCERT/CC will publish these reports in a timely manner to communicate relevant information to everyone involved in information security at companies and other organizations, with a view to helping prevent incidents and accelerating their resolution.

The first Incident Response Report, which was issued in June 2017, was translated and posted on JPCERT/CC's English blog, entitled "What the Avalanche Botnet Takedown Revealed: Banking Trojan Infection in Japan" It introduced activities undertaken by JPCERT/CC in the global effort to dismantle the Avalanche botnet, as well as the current status of malware-infected devices in Japan related to the Avalanche botnet.

What the Avalanche Botnet Takedown Revealed: Banking Trojan Infection in Japan
http://blog.jpcert.or.jp/2017/08/what-the-avalanche-botnet-takedown-revealed-banking-trojan-infection-in-japan.html