JPCERT/CC®

Japan Computer Emergency
Response Team Coordination
Center

電子署名者 : Japan Computer Emergency Response Team
Coordination Center
DN : c=JP, st=Tokyo, l=Chiyoda-ku,
email=office@jpcert.or.jp, o=Japan Computer Emergency
Response Team Coordination Center, cn=Japan Computer
Emergency Response Team Coordination Center
日付 : 2015.09.08 09:39:56 +09'00'

JPCERT-PR-2015-03
Issued: 2015-07-14

JPCERT/CC Activities Overview [April 1, 2015 – June 30, 2015]

Activity Overview Topics

－Topic 1－ Contacted 66 organizations to alert of possible advanced cyber attacks

During this quarter, JPCERT/CC notified 66 organizations of the possibility that they were being subjected to advanced cyber attacks including targeted attacks. Of these, 44 were contacted regarding remote control malware called Emdivi. Emdivi has been used to carry out attacks against a large number of domestic organizations over an extended period of time. Organizations that were infiltrated into their internal network have reported unauthorized access to their Active Directory servers and file servers, resulting in damages such as leakage of various information including personally identifiable information.

JPCERT/CC has conducted investigations on the malware used and the attack base (C&C servers, etc.) that it communicates with, based on incident reports, etc., regarding targeted attacks. The information obtained through the investigation has been used to provide information to other organizations that might become a target of attack, and to contact and alert organizations that are presumed to be actually subjected to attack. Information about attack base and attack method obtained by JPCERT/CC through its investigations is aggregated and provided to aid the initial actions that are conducted by each organization in order to comprehend the status of infiltration, including the analysis of log data and identification of infected terminals.

This type of attack is carried out persistently using different methods even after it becomes known, and affected servers may remain accessible to attackers. Therefore, it is imperative that appropriate initial actions are taken early on to prevent the spread of damages. If alerts of an attack are received from an external source, verify the facts, consult with a security vendor, and then take measures to prevent the spread of damages and investigate the scope of impact on the entire organization. Please contact JPCERT/CC if there is any uncertainty regarding initial actions such as the verification of facts.

Notification of incidents related to targeted attacks
https://www. jpcert.or.jp/incidentcall/

"Targeted attack" has been added as a new category item for the number of incidents in the Incident Handling Report. JPCERT/CC updates its Incident Handling Status on its website every day. Please refer to our quarterly reports for official statistical information.

Incident Handling Status

https://www.jpcert.or.jp/ir/status.html

－Topic 2－ Council of Anti-Phishing Japan celebrates 10-year anniversary

The Council of Anti-Phishing Japan, founded on April 28, 2005, has marked its 10-year anniversary. As of June 1, 2015, its membership encompasses 81 organizations (23 full members, 48 supporting members, 3 research partners, and 7 observers). After the general assembly of the Council in June, a celebration was held to commemorate the milestone.

Congratulatory speeches were given by guests from the Ministry of Economy, Trade and Industry and the National Police Agency, and participating members actively exchanged opinions on future operations and activities of the Council. During the celebration, the working group in charge announced the opening of a new Facebook page for the "Stop.Think.Connect. (STC)" campaign, which is being pursued by the Council of Anti-Phishing Japan in cooperation with its overseas counterparts, and is aimed at raising awareness of cyber security risks in individuals. Going forward, the Council of Anti-Phishing Japan will actively use its website as well as Facebook, etc., to further promote its educational activities.

Council of Anti-Phishing Japan (Japanese)

https://www.antiphishing.jp/

Stop.Think.Connect. (STC) Official Website (Japanese)

http://stopthinkconnect.jp/

Stop.Think.Connect. Facebook Page (Japanese)

https://www.facebook.com/StopThinkConnectJapan