Topic I: Measures to Prevent Cybercrime/Cyber-Attack Damage

With an increasing prevalence, complexity and sophistication of the modus operandi of cybercrimes and cyber-attacks, the importance of damage prevention measures is also increasing. The police are actively sharing information on the modus operandi of such cybercrimes and cyber-attacks and are also promoting various damage prevention measures in collaboration with private business operators and overseas investigation agencies.

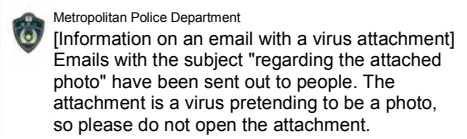
(1) Information Dissemination by the Police

The police are asking for the public to be more cyber aware by actively disseminating information on the modus operandi of cybercrimes and cyber-attacks that the police have gathered in the course of criminal investigations. The National Police Agency (NPA) posts information on the current status and modus operandi of cybercrimes and cyber-attacks on the NPA's portal site developed for ensuring that the Internet environment of general users becomes secured, reminding them to be wary of cybercrimes and to take appropriate damage prevention measures. In addition to these efforts, prefectural police are also disseminating information through their websites, SNS and other means of communication to prevent cybercrime and cyber-attack damage.

Cyber Police Agency

[Case] In October 2016, the Cyber Force Center of the NPA alerted the public of the spread of a virus called Mirai that is a malicious program that targets devices connected to the Internet such as household appliances including digital video recorders and web cameras.

[Case] In October 2016, the Metropolitan Police Department (MPD) analyzed one of the malicious programs that distributes emails with a virus related to illegal money transfer and developed a system that detects such virus at the stage when the command server of the malicious program orders the computer infected with the same malicious program to send the emails infected with the virus. Since November of the same year, the NPA and the MPD have been disseminating such information, such as the subject of email with the virus, through SNS and other means of communication.



An Example of Information Disseminated via SNS

(2) Efforts through Public-Private Collaboration

In order to prevent damage arising from cybercrimes and cyber-attacks, it is important to work collaboratively with private business operators. Working in collaboration with the Japan Cybercrime Control Center (JC3), the police are disseminating information to prevent damage and are also taking various damage prevention measures through public-private collaboration, such as conducting joint prevention drills with business operators which could be targets of cyber-attacks in the future.

[Case] From May to July 2016, the Tokushima Prefectural Police and other police forces have obtained information on a malicious program created for stealing the online banking information of individuals, such as IDs, passwords and credit card numbers, in the course of their criminal investigation on illegal money transfers via online banking. On the basis of this information, the NPA conducted a joint analysis with the JC3 and identified the infection route and other details of the malicious program. In June of the same year, the NPA, in collaboration with an overseas investigation agency, brought down the command and control server connected to the computer infected with the same malicious program. The JC3 also released a warning about the malicious program on its website, asking Internet users to take appropriate measures.

[Case] The Saitama Prefectural Police, setting their sights on the Tokyo 2020 Olympic and Paralympic Games, conducted a joint drill, as part of measures against cyber-attacks, in March 2016 with administrators of facilities which would be venues of the Games. In the drill, assuming that a computer used by a member of staff of the facility was infected with a malicious program due to a cyber-attack, participants of the drill checked on procedures for responding to the incident. The police, demonstrating how a computer infected with the malicious program could be controlled remotely, highlighted the seriousness of cyber-attacks.

At the Joint Cyber Security Drill

(3) Efforts through Collaboration with Overseas Investigation Agencies

Global efforts are needed to combat the threat of cyberspace and the police are making various efforts to prevent damage arising from cybercrimes and cyber-attacks by always working closely with overseas investigation agencies.

[Case] In order to prevent damage arising from websites which were hosted on overseas servers, and which were disguised as those of actual companies or were opened to commit online shopping fraud or to sell counterfeit name brand goods, the NPA, since July 2016, has begun providing information, obtained in the course of investigation, on those websites for the Anti-Phishing Working Group (APWP) that many web browser companies have joined as well as for antivirus software companies. These efforts have enabled computer screens of Internet users who do not install antivirus software to display a warning message when they are about to browse these malicious websites.

[Case] In November 2016, as the malicious program suspected to be used in illegal money transfers via online banking is spreading throughout the world, investigation agencies of countries concerned to which Germany was central worked together to arrest the suspects of illegal money transfers where the malicious program was used, and also seized their command servers. On the basis of the information provided by investigation agencies in Germany and other countries, the NPA, in collaboration with related agencies and organizations, is encouraging online banking users to change their IDs and passwords that were stolen by this malicious program. Also, the NPA is providing information on how to remove such program to computer users in Japan whose computers have been infected with the program.

Overview of Global Measures to Prevent Damage from Illegal Money Transfers Committed via Online Banking