UNOFFICIAL TRANSLATION

Press release
September 7th, 2017
National Police Agency

The situation of threats in cyberspace in the first half of 2017

1. Cyber attacks

(1) Scanning activities in cyberspace

- The number of unexpected incoming packets in a day to the sensors deployed at the Internet connection point was 2,008.4 per IP address, decreasing by 250.2 compared to the second half of 2016. While this is a decrease of 10% from the second half of 2016, the number of the packets was approximately twice compared to the first half of 2016.
- The main reason for the decrease of unexpected incoming packets compared to the second half of the 2016 was a decrease of scanning activities by "Mirai" bots. However, the scanning activities were still observed.
- Not only infection activities by ransomware "WannaCry" which caused damage on a world scale, but also cyber-attacks where exploits which were abused in the "WannaCry" case were utilized were observed.

(2) Situation of cyber-attacks and cybersecurity measures

a. Situation

- Cyber-attacks were occurring all over the world in 2017 as well as in 2016.
- The number of spear phishing e-mail attacks the Japanese police confirmed in the first half of 2017 was 589 cases, decreasing by 1,506 cases compared to the second half of 2016. As for the format of files attached to spear phishing e-mails, the police found out file formats which had rarely been reported before, and also found the proportion of each file format had been changed.
- The Japanese police confirmed that a self-styled international hacker group "Anonymous" posted messages on SNS which were believed to be claims of responsibility for the cyber-attacks against 60 organizations.

b. Efforts

- The Japanese police prompted hosting service providers to stop the function of 43 domestic C2 servers (the number increased by 15 compared to the preceding half year) which the police found through the analysis of malware used in cyber-attack cases.
- Preparing for the Tokyo 2020 Olympic and Paralympic Games, the Japanese police conducted several measures against cyber-attacks, such as joint exercises with relevant organizations and sharing information therewith.

2. Cybercrimes

(1) Situation

The number of cleared cybercrime cases decreased by 71 to 4,209 compared to the first half of 2016. And the number of consultation regarding possible cybercrimes increased by 3,238 to 69,977 compared to the first half of 2016. The number of consultations was the highest-ever.

(2) Online banking fraud

- The number of online banking fraud cases decreased by 645 to 214 and the total amount of damage due to the online banking fraud decreased by about 333 million yen (2.9 million US dollars) to about 564 million yen (5 million US dollars) compared to the first half of 2016.
- The online banking fraud in the first half of 2017 was characterized by the great decrease in damage to personal accounts of financial institutions, on the other hand, the new modus operandi where a remittance to virtual currency exchangers with electronic payment systems emerged.

(3) Online banking fraud by unauthorized access to virtual currency account

- The number of reported cases was 23, and the total amount of damage was about 59.2 million yen (524 thousand US dollars). The number of reported cases increased sharply in and after May 2017.
- Though every virtual currency exchanger which suffered unauthorized access had introduced two-step authentication, 20 victims of unauthorized wire transfer (87.0%) did not make use of the two-step authentication.

(4) Efforts

- Taking measures against leaked IDs and infected computers which were identified in the international endeavor "Operation Avalanche."
- Taking measures, with public-private partnership, against falsification of websites intended to infect computers.
- Taking measures against "DreamBot," an online banking malware, which has a function to get an infected computer transferring money, without notice, from an account whose holder is a user of the infected computer to another.
- Requesting administrating organizations of an electronic payment system and virtual currency exchangers to enhance monitoring, to promote use of one-time password, and to implement customer identity verification thoroughly.

3. Future initiatives

On the basis of the "Cybersecurity Strategy of the Japanese Police" dated September 4th, 2015, the Japanese police promote various initiatives or measures including the following;

- Promoting information gathering and analysis concerning cyber space.

- Promoting partnership between the public and private sectors.
  - Partnership with the Japan Cybercrime Control Center (JC3), a private foundation
    - Information sharing for ensuring the cyber space security
    - Measures for preventing further damage, with public-private partnership, by disseminating information
  - Partnership with critical infrastructure providers, business operators with cutting-edge technology, and others businesses
- Human resource development for cybersecurity.
  - Developing specialized investigators (including enhancement of education and training in the Cybersecurity Research and Training Center)
  - Developing highly professional human resources for digital forensics
- International collaboration.
  - Collaboration with foreign law enforcement agencies
- Promoting cybersecurity measures for the Tokyo 2020 Olympic and Paralympic Games (including information sharing and joint exercises with relevant organizations).

(End)

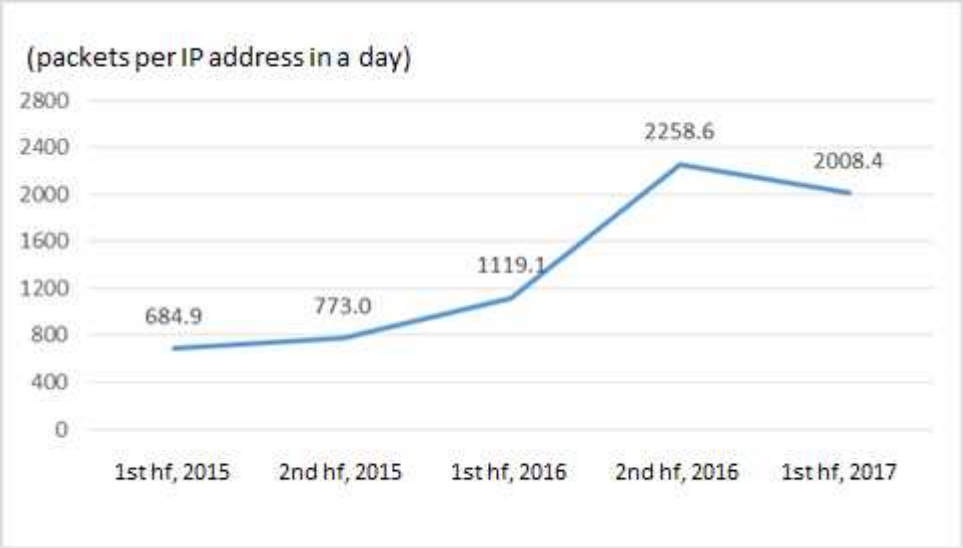
The situation of threats in cyberspace in the first half of2017

1. Cyber-attacks

(1) Scanning activities in cyberspace

a. Overview of unexpected incoming packets to the sensors[1]

The number of unexpected incoming packets to the sensors was 2,008.4 per IP address in a day, decreasing by 250.2 compared to the second half of 2016.



[Number of unexpected incoming packets to the sensors]

b. Characteristics

- Scanning activities targeting IoT devices.

Though the number of unexpected incoming packets which seemed to be scanning or infection activities by bots, "Mirai" (and its variants) targeting IoT devices increased sharply in 2016, the number in a day in the second half of 2017 was 494.3 per IP address, decreasing by 386.3 compared to the second half of 2016.

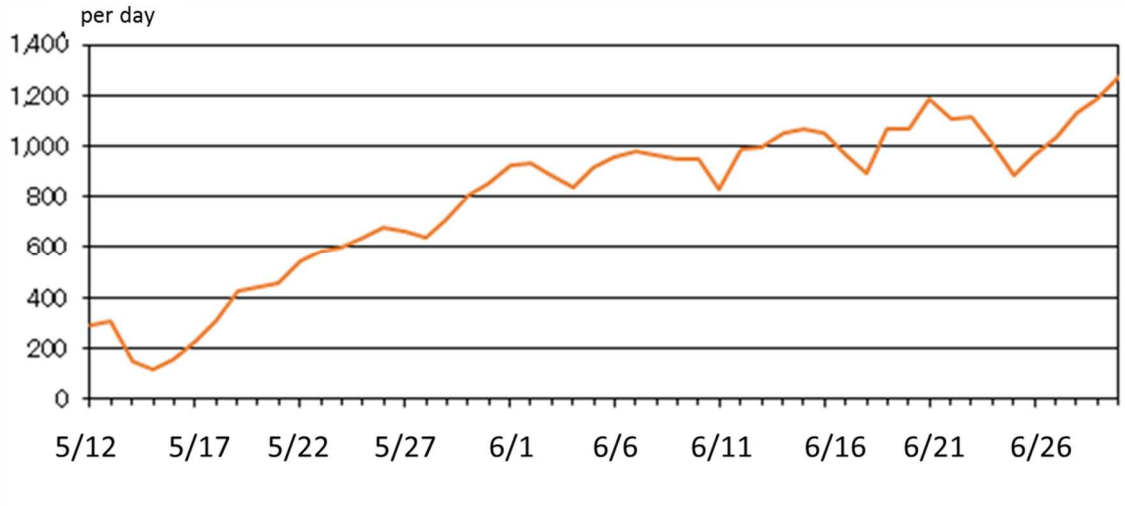
- Infection activities of ransomware "WannaCry."

In April, exploits "Eternalblue" and "Doublepulsar" whose target was Microsoft Windows were leaked to the public by a group calling themselves "Shadow Brokers," and scanning activities or cyber-attacks targeting infected devices by the exploits were observed thereafter.

In May, ransomware "WannaCry" spread worldwide, and the National Police Agency (NPA) observed its activities of infection. WannaCry was malware to exploit "Eternalblue" and "Doublepulsar." In June, the NPA confirmed that infection of WannaCry's variants was

[1] The sensors are components of the Real-time Detection Network System that the NPA operates around-the-clock, and are placed at the Internet connection points. These sensors detect connecting information (including scanning activities for trying cyber-attacks) which is not assumed to be ordinary use of the Internet, and the System assembles and analyzes the information.

spreading, though users of computers where the variants were infected rarely noticed the infection.



[Transitions of number of access to port 445/TCP, which is characteristic of infection activity of WannaCry]

- Scanning activities targeting vulnerabilities of Apache Struts 2.[2]

The NPA observed scanning activities and cyber-attacks targeting critical vulnerabilities of Apache Struts 2, which were announced one after another in March.

(2) Situation of cyber-attacks and efforts toward them

a. Situation

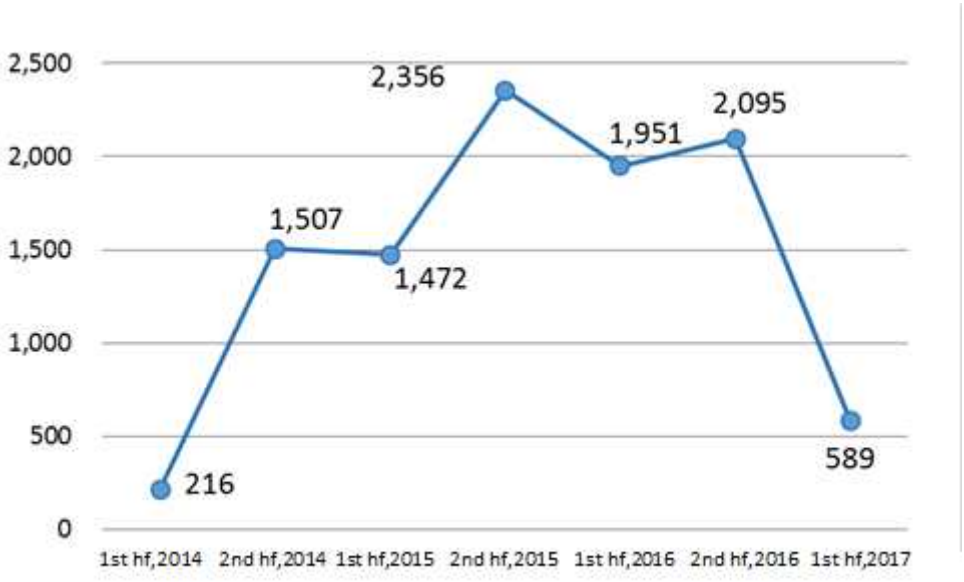
(a) Overview

The Japanese police shared information on cyber-attacks which seemed to intend to thieve information with business operators through the Counter Cyber-intelligence Information-Sharing Network[3]. The number of spear phishing e-mail attacks the Japanese police confirmed through the network in the first half of 2017 was 589 cases, decreasing by 1,506 cases compared to the second half of 2016.

As for formats of the files attached to spear phishing e-mails, file formats which had rarely been reported before were found out, and there was also a tendency that the percentage of the file formats tended to be different from before.

[2] Apache Struts 2 aims to improve the efficiency of application development, providing functions widely used for development of web applications written in Java script.

[3] A framework between the police and 7,613 organizations/business operators with cutting-edge technologies all over the country (as of July 2017) to share information on cyber-attacks which seem to intend to thieve information. Through the framework the police and the member organizations/business operators also share results of analysis on spear phishing e-mail attacks against governmental entities, in coordination with the National Center of Incident-readiness and Strategy for Cybersecurity (NISC).



[Number of spear phishing e-mail attacks]

[Mechanism of spear phishing e-mail attacks]

And browsing failure in the websites of Japanese government agencies, airports and aquariums occurred as in 2016.

The Japanese police confirmed that a self-styled international hacker group "Anonymous" posted messages on SNS which seemed to be claims of responsibility for the cyber-attacks against 60 organizations.

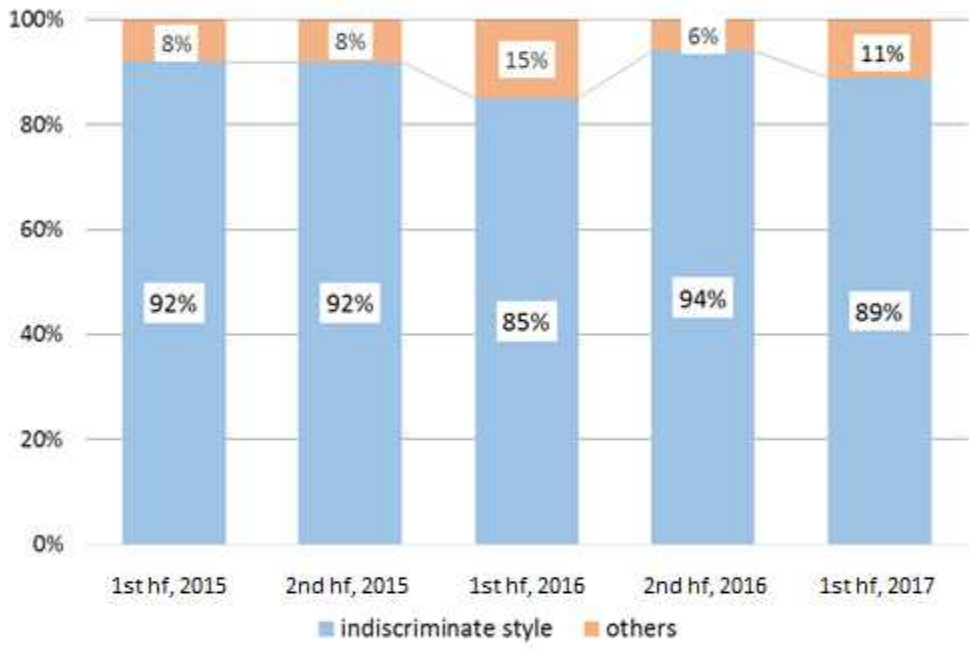
(b) Modus operandi of spear phishing e-mail attacks

- "Indiscriminate style"[4] spear phishing e-mail attacks occurred.

A lot of "indiscriminate style" spear phishing e-mail attacks occurred as in 2016. The

[4] The NPA defines an act intending to thieve information by sending e-mails which are disguised as what is related to business of an addressee and authentic with malware which cannot be detected by commercially available anti-virus software, and by infecting a computer of the addressee with the malware as "spear phishing e-mail attack." The NPA counts the spear phishing e-mail attack where e-mails with the same text or the same malware are sent to 10 or more than 10 addressees in "indiscriminate style."

“indiscriminate style” spear phishing e-mail attacks accounted for about 90 % of the total.



[Percentage of “indiscriminate style” spear phishing e-mail attacks and others]

- Most of the spear phishing e-mails were sent to unpublicized e-mail addresses.

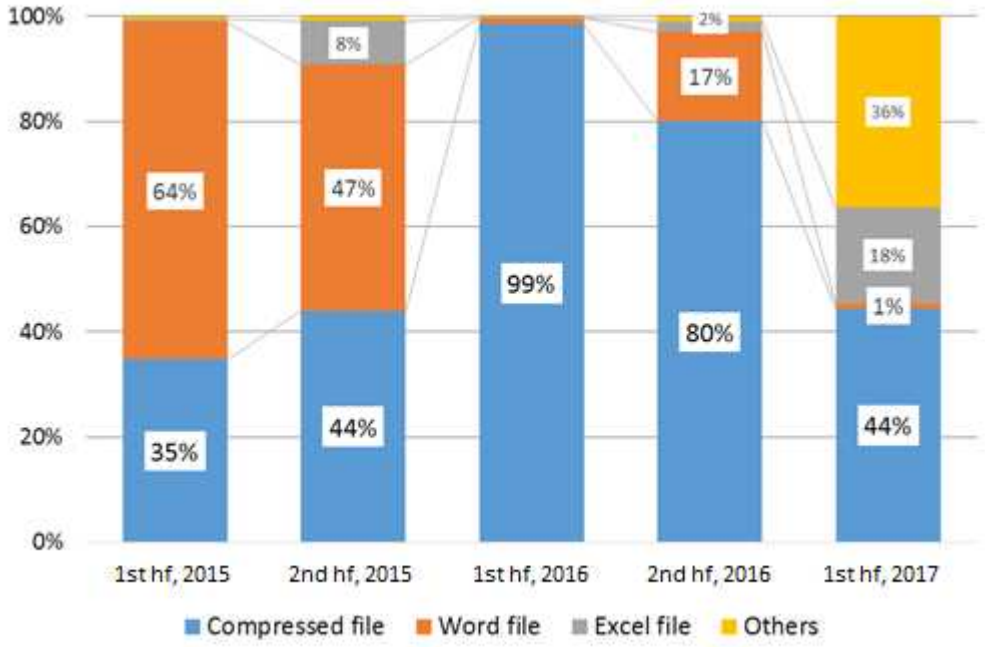
As for destination of spear phishing e-mails, unpublicized e-mail addresses accounted for about 96% of the total. The percentage is high as in 2016.

- E-mail addresses of most of spear phishing e-mails were forged.

Almost all e-mail addresses of spear phishing e-mail senders were forged. The senders of these e-mails pretended to be reliable institutions such as universities and banks. These e-mail addresses which seemed to be forged accounted for 99% of the total.

- Change in formats of files which were attached to spear phishing e-mails.

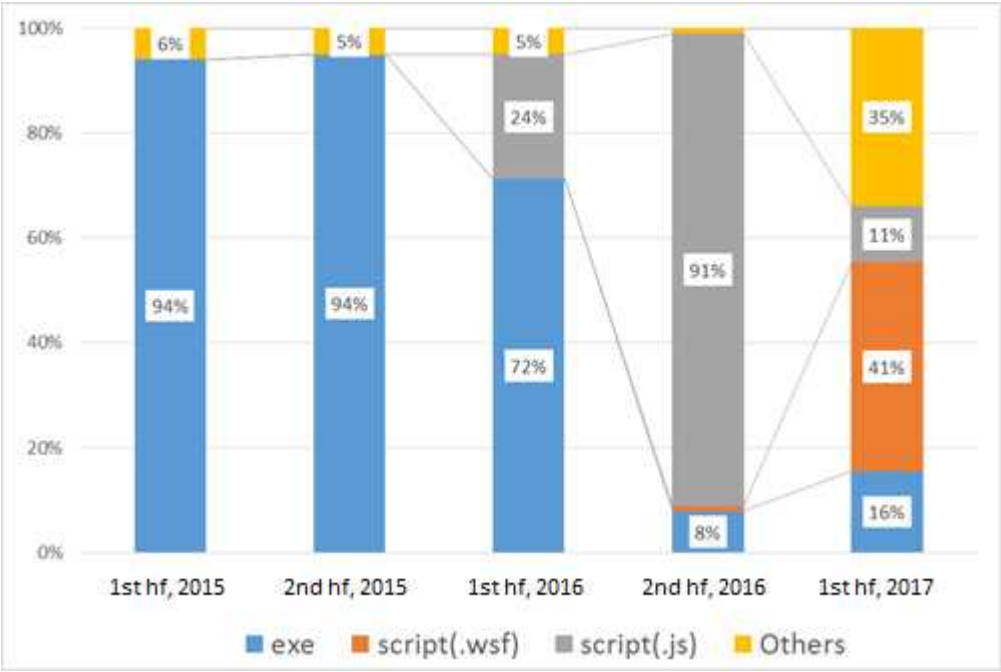
Though files of the MS-Word format had been likely to be attached to spear phishing e-mails, the number of the spear phishing e-mails where MS-Word files themselves were attached decreased in the first half of 2017. PDFs where MS-Word files were embedded were newly found out. Formats of files which are attached to spear phishing e-mails changed as countermeasures against these e-mails prevail. It seems that countermeasures against spear phishing e-mails where an MS-Word file itself is attached have prevailed to a certain extent.



[Percentage of the file formats of spear phishing e-mail attachments]

- Change in formats of files which were compressed.

As for formats of files which were compressed, the proportion of ".js" files which were found out in the second half of 2016 decreased, and that of ".wsf" files increased. In recent years, script files have been used frequently. In the first half of 2017, the sum of the proportion of ".js"files and ".wsf"files accounted for about 50% of the total. It seems that use of script files has expanded, and that kinds of them have been diversified.



[File formats of the compressed files]

b. Efforts

(a) Takedowns on C2 servers used for cyber-attacks

The Japanese police encouraged hosting server businesses to take down C2 servers[5] which had been identified through the analysis of malware used in cyber-attack cases. Forty three C2 servers were taken down in the first half of 2017, and the number exceeded 28, the number in the second half of 2016.

(b) Promoting countermeasures against cyber-attacks on the Tokyo 2020 Olympic and Paralympic Games.

Preparing for the Tokyo 2020 Olympic and Paralympic Games, the Japanese police conducted several measures against cyber-attacks, such as joint exercises with relevant organizations on the supposition of cyber-attacks and information sharing with relevant organizations in the countries that had hosted the Olympic Games before.

(c) Enhancing dissemination of information

The NPA had disseminated information about cybersecurity at the section of "@police" and "Countermeasures against Cybercrime" (that "Project for Countermeasures against Cybercrime" has replaced since June 26) on the website of the NPA. Furthermore the NPA has enhanced dissemination of information since June 26, opening the portal site "Cyber Police Agency" (http://www.npa.go.jp/cybersecurity/) where information of "@police" and "Countermeasures against Cybercrime" has been integrated.

2. Cybercrimes

(1) The number of cleared cybercrime cases and consultation regarding cybercrime

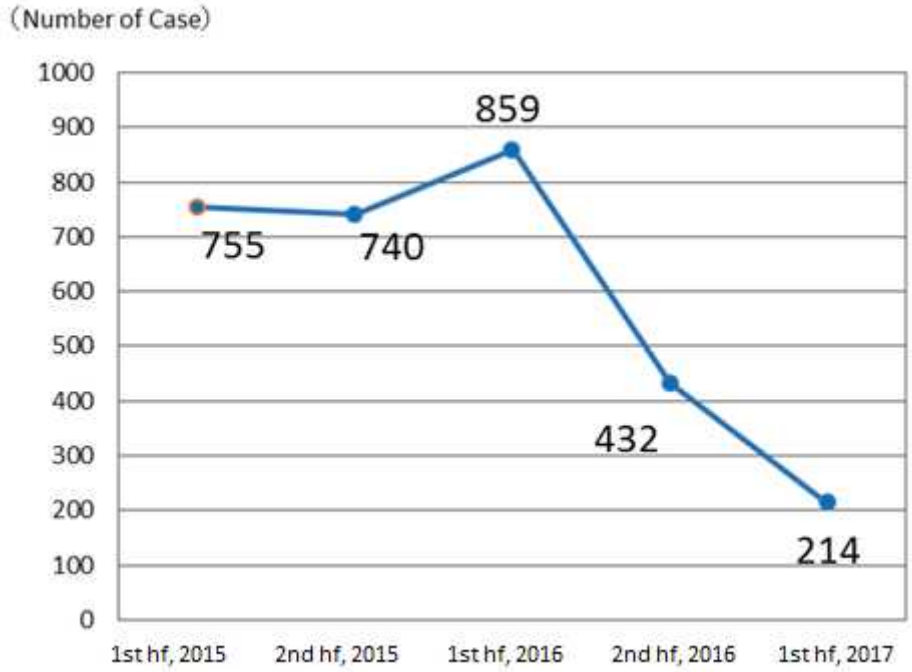
The number of cleared cybercrime cases was 4,209, decreasing by 71 (1.7%) compared to the first half of 2016. And the number of consultation regarding cybercrime was 69,977, increasing by 3,238 (4.9%) compared to the first half of 2016. The number of consultations is the highest-ever on a half-year basis.

(2) Online banking fraud

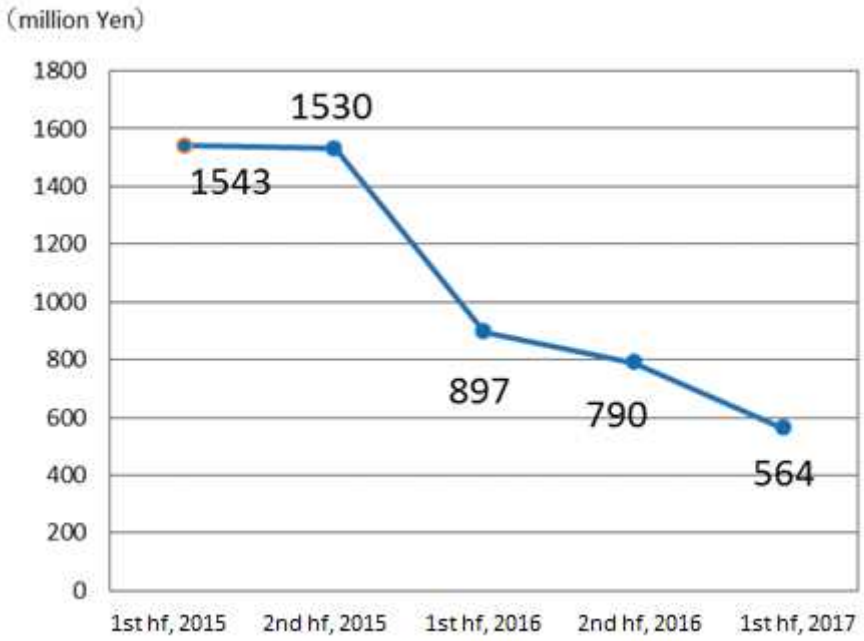
a. Overview

The number of online banking fraud cases was 214, decreasing by 645 compared to the first half of 2016, and the amount of damage was about 564 million yen (5 million US dollars), decreasing by about 333 million yen (2.9 million US dollars) compared to the first half of 2016. The decrease was due to a decrease in the cases concerning personal accounts opened in financial institutions.

[5] Standing for "command and control server." It might be abbreviated to "C and C server." C2 servers are the center of control, giving commands to a computer which is infected with malware operating in response to the commands.



[Number of online banking fraud]



[Amount of damage of online banking fraud]

b. Characteristics

- Significant decrease in the amount of damage concerning personal accounts opened in financial institutions.

The amount of damage concerning personal accounts opened in financial institutions decreased by about 513 million yen (4.5 million US dollars) compared to the first half of 2016.

- Significant decrease in the amount of damage concerning personal account at the major commercial banks.

The amount of damage concerning personal account at the major commercial banks decreased by about 464 million yen (4.1 million US dollars) compared to the first half of 2016. It seemed that the decrease was due to preventive measures, including enhancement of monitoring[6], taken by these banks.

- Occurrence of new type of online banking fraud, abusing electronic settlement service system.

A new modus operandi, where a remittance to virtual currency exchangers was carried out through electronic settlement service system of online banking, appeared.

Virtual currency equivalent to about 69 million yen (611 thousand US dollars) out of that equivalent to about 104 million yen (920 thousand US dollars) which was remitted to the virtual currency exchangers by means of this modus operandi was frozen at the virtual currency exchangers (The value of the virtual currency is converted to yen at the rate in July 2017).

- About 50% of destination accounts for unauthorized wire transfer were under names of Vietnamese.

As for nationalities of account holders, Vietnam represented 51%, China 23%, and Japan 11% of 374 accounts which were identified as first destination accounts for unauthorized wire transfer.

(3) Online banking fraud by unauthorized access to virtual currency account

- The number of the reported cases was 23, and the amount of damage was equivalent to about 59.2 million yen (524 thousand US dollars). The number of the reported case increased sharply in and after May this year.
- Though every virtual currency exchanger which was the subject of unauthorized access had introduced two-step authentication,[7] 20 victims of unauthorized wire transfer (87%) out of 23 did not make use of two-step authentication.

(4) Efforts

- Measures against leaked IDs and infected computers which were found out in the international effort “Operation Avalanche.”

The international effort “Operation Avalanche” helped the Japanese police acquire information on leaked IDs and passwords of online banking users and information on virus-infected computers, and the Japanese police, cooperating with ministries, agencies and other organizations, urged the users of the online banking and the virus-infected computers to draw

[6] Enhancing to monitor IP addresses which were used for unauthorized remittance.
[7] Requiring further recognition by a one-time password, etc. in addition to general identification code (IDs and passwords).

attention to prevent further damage.

- Measures, with public-private partnership, against tampering with websites to infect computers.

The Chiba Prefectural Police, forming a partnership with the JC3 (Japan Cybercrime Control Center) analyzed information provided by the JC3. They established a technique to confirm authenticity of websites. And 38 prefectural police provided guidance for website administrators.

- Countermeasures against "DreamBot" which is malware with function to remit balance without being noticed by account holders.

The Metropolitan Police Department, forming a partnership with the JC3, elucidated the function of the online banking malware "DreamBot," and urged Internet users and financial institutions to draw attention. And the JC3 created on its website the web page where Internet users could check whether their computers were infected with "DreamBot."

- Providing information leading directly to prevention of damage, and requesting to enhance preventive measures.

The NPA requested financial institutions, an electronic settlement service system management organization and virtual currency exchangers to enhance monitoring, urge their customers to use one-time password and two-step authentication, and implement thoroughly customer identification.

(End)