Machine Learning and Security

1.1 Introduction

This report summarizes incidents to which IIJ responded, based on general information obtained by IIJ itself related to the stable operation of the Internet, information from observations of incidents, information acquired through our services, and information obtained from companies and organizations with which IIJ has cooperative relationships. This volume covers the period of time from April 1 through June 30, 2015. In this period a number of hacktivism-based attacks were once again carried out by Anonymous and other groups, and there was a rash of attacks including SNS account hijackings and website defacements. There were also many incidents of malware infection through targeted attacks, and it was identified that the personal information of as many as 1.25 million people may have leaked in incidents affecting the Japan Pension Service. Information leaks caused by unauthorized access also continue to occur, including an incident in which the U.S. Office of Personnel Management was breached, leading to the leak of information on roughly 4 million employees. These examples show that many security-related incidents continue to occur on the Internet.

1.2 Incident Summary

Here, we discuss the IIJ handling and response to incidents that occurred between April 1 and June 30, 2015. Figure 1 shows the distribution of incidents handled during this period*1.

The Activities of Anonymous and Other Hacktivists

Attacks by hacktivists such as Anonymous continued during this period. DDoS attacks and information leaks occurred at government-related and corporate sites in a large number of countries stemming from a variety of incidents and causes.

Individuals and organizations thought to be associated with ISIL or sympathetic to its principles carried out website defacements and SNS account hijackings around the world. In April, a French TV station was targeted in a large-scale attack, interrupting the broadcast of programs. At the same time as the attack that compromised the station's internal system*2, its SNS accounts such as Facebook and Twitter were hijacked and unauthorized posts made. In opposition to this, Anonymous continued publishing lists of websites and SNS accounts thought to be connected to ISIL, and encouraging their suspension or deletion (OpISIS). There was also ongoing confusion, including a group that had been active as a Palestinian branch of Anonymous being targeted in attacks by other Anonymous factions, who accused them of supporting ISIL.

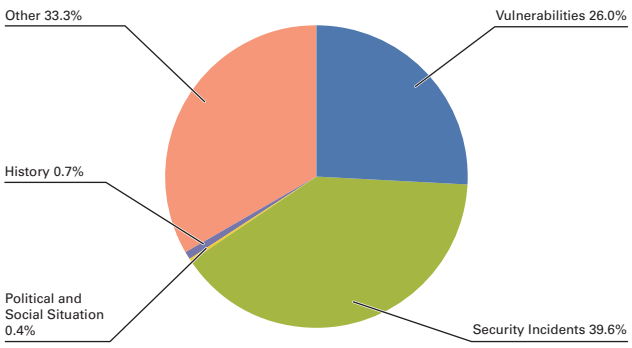


Figure 1: Incident Ratio by Category (April 1 to June 30, 2015)

In protest against airstrikes in Yemen carried out by the government of Saudi Arabia, among other reasons, there were DDoS attacks on Saudi Arabian newspaper companies, and leaks of confidential information caused by server compromises targeting a number of government agencies (OpSaudi). Additionally, in opposition to the bombing of Gaza

*1 Incidents discussed in this report are categorized as vulnerabilities, political and social situations, history, security incidents or other.
Vulnerabilities: Responses to vulnerabilities associated with network equipment, server equipment or software commonly used over the Internet or in user environments.
Political and Social Situations: Responses to incidents related to domestic and foreign circumstances and international events such as international conferences attended by VIPs and attacks originating in international disputes.
History: Historically significant dates; warning/alarms, detection of incidents, measures taken in response, etc., related to attacks in connection with a past historical fact.
Security Incidents: Unexpected incidents and related responses such as wide propagation of network worms and other malware; DDoS attacks against certain websites.
Other: Security-related information, and incidents not directly associated with security problems, including highly concentrated traffic associated with a notable event.

*2 It has been pointed out that a RAT may have been used in these attacks. Trend Micro, "Kjw0rm VBS Malware Tied To Attacks on French TV Station TV5Monde" (http://blog.trendmicro.com/trendlabs-security-intelligence/vbs-malware-tied-to-media-attacks/).

by Israel, there were ongoing attacks resulting in the leak of personal and credit card information due to incidents of unauthorized access at a number of Israeli companies (OpIsrael), etc. As this demonstrates, Internet-based attacks also continue to occur in Middle-Eastern countries due to conflicts and diplomatic circumstances.

In Canada, there were a number of DDoS attacks as well as website defacements and leaks of internal information due to server compromises targeting a number of government agencies (OpC51). These were related to the passing of an Anti-terrorism Act in June that significantly expands and strengthens the authority of the Canadian Security Intelligence Service, triggering privacy concerns. In India, there were DDoS attacks and also leaks of account information caused by unauthorized access targeting a number of government agencies, including the Telecom Regulatory Authority of India, in protest against government moves to bolster Internet regulations. In Japan, there were reports of incidents of unauthorized access in May thought to be carried out by Anonymous to protest against the commercial use of marine animals such as whales and dolphins (OpSeaWorld). These led to the leak of registrant information such as email addresses from the Japanese Association of Zoos and Aquariums (JAZA).

Unknown attackers claiming affiliation with the Syrian Electronic Army continued to hijack accounts and deface websites, with affected organizations including U.S. newspaper company the Washington Post, as well as the U.S. Army. Other attacks by hacktivists such as Anonymous continued on government and government-related sites around the world, such as in Italy, Brazil, and China. There were also ongoing hijacking incidents targeting prominent SNS accounts, such as those of government institutions.

■ Vulnerabilities and their Handling

During this period fixes were released for Microsoft's Windows*3*4*5*6*7, Internet Explorer*8*9*10, and Office*11. Fixes were also released for Adobe Systems' Adobe Flash Player. A quarterly update was provided for Oracle's Java SE, fixing many vulnerabilities. Additionally, because support for Java 7 is scheduled to end as of this update, migration to Java 8 is recommended. Several of these vulnerabilities were exploited in the wild before patches were released.

Regarding server applications, a quarterly update was released for a number of Oracle products, including the Oracle database server, fixing many vulnerabilities. An XSS vulnerability in multiple versions of the WordPress CMS that could allow arbitrary code execution was discovered and fixed. An XSS vulnerability was also discovered and fixed in a WordPress plug-in*12. A vulnerability that could allow remote code execution due to insufficient checking of entered values was discovered in fixed in the Movable Type CMS*13.

*3 "Microsoft Security Bulletin MS15-034 - Critical: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)" (https://technet.microsoft.com/en-us/library/security/ms15-034.aspx)
*4 "Microsoft Security Bulletin MS15-035 - Critical: Vulnerability in Microsoft Graphics Component Could Allow Remote Code Execution (3046306)" (https://technet.microsoft.com/en-us/library/security/ms15-035.aspx).
*5 "Microsoft Security Bulletin MS15-044 - Critical: Vulnerabilities in Microsoft Font Drivers Could Allow Remote Code Execution (3057110)" (https://technet.microsoft.com/en-us/library/security/ms15-044.aspx).
*6 "Microsoft Security Bulletin MS15-045 - Critical: Vulnerability in Windows Journal Could Allow Remote Code Execution (3046002)" (https://technet.microsoft.com/en-us/library/security/ms15-045.aspx).
*7 "Microsoft Security Bulletin MS15-057 - Critical: Vulnerability in Windows Media Player Could Allow Remote Code Execution (3033890)" (https://technet.microsoft.com/en-us/library/security/ms15-057.aspx).
*8 "Microsoft Security Bulletin MS15-032 - Critical: Cumulative Security Update for Internet Explorer (3038314)" (https://technet.microsoft.com/en-us/library/security/ms15-032.aspx).
*9 "Microsoft Security Bulletin MS15-043 - Critical: Cumulative Security Update for Internet Explorer (3049563)" (https://technet.microsoft.com/en-us/library/security/ms15-043.aspx).
*10 "Microsoft Security Bulletin MS15-056 - Critical: Cumulative Security Update for Internet Explorer (3058515)" (https://technet.microsoft.com/en-us/library/security/ms15-056.aspx).
*11 "Microsoft Security Bulletin MS15-033 - Critical: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3048019)" (https://technet.microsoft.com/en-us/library/security/ms15-033.aspx).
*12 See the following blog post from U.S. security firm Sucuri for more information. "Security Advisory: Persistent XSS in WP-Super-Cache" (https://blog.sucuri.net/2015/04/security-advisory-persistent-xss-in-wp-super-cache.html).
*13 Six Apart, "MOVABLE TYPE 6.0.8 AND 5.2.13 RELEASED TO CLOSE SECURITY VULNERABILITY" (https://movabletype.org/news/2015/04/movable_type_608_and_5213_released_to_close_security_vulnera.html).

April Incidents

S **1st: A number of reports were published indicating that large-scale DDoS attacks on GitHub that occurred in March were related to transmissions to China.**
See the following NETRESEC announcement for more information on these attacks. "China's Man-on-the-Side Attack on GitHub" (http://www.netresec.com/?page=Blog&month=2015-03&post=China%27s-Man-on-the-Side-Attack-on-GitHub). Security researcher Robert Graham has also looked into where the MITM attacks were being carried out in the following report. "Pin-pointing China's attack against GitHub" (http://blog.erratasec.com/2015/04/pin-pointing-chinas-attack-against.html#.VahhVfntnK4).

S **8th: It was announced that member information registered on a service site for stockholders used by a number of listed companies may have leaked.**
This incident was uncovered when investor solicitation was carried out by email and phone based on the information that had leaked. Upon later investigation it was announced that this was an inside job rather than being caused by unauthorized access.

O **8th: The FBI issued an alert due to a series of website defacements exploiting vulnerabilities in WordPress plug-ins that were carried out by someone claiming affiliation with ISIL.**
The Internet Crime Complaint Center (IC3), "ISIL DEFACEMENTS EXPLOITING WORDPRESS VULNERABILITIES" (http://www.ic3.gov/media/2015/150407-1.aspx).

S **9th: French TV network the TV5MONDE group was accessed without authorization by someone claiming affiliation with ISIL, leading to damages including the hijacking of websites and SNS site accounts. Other impact from these attacks included the interruption of TV broadcasts for seven hours.**
"Press release from April 9th 2015"
(https://asia.tv5monde.com/Resources/Articles/Events/2015/04-en/Press-release-from-April-9th-2015?lang=en-US).

S **10th: The European Police Office (Europol) announced they had taken down the Beebone botnet (also known as AAEH, etc.) together with investigative organizations and security firms in various countries, including the Federal Bureau of Investigations (FBI).**
"International Police Operation Targets Polymorphic BEEBONE Botnet"
(https://www.europol.europa.eu/content/international-police-operation-targets-polymorphic-beebone-botnet).

S **10th: The Tokyo Metropolitan Police Department initiated a takedown of malware related to Internet banking in Japan (VAWTRAK), in collaboration with the Ministry of Internal Affairs and Communications, Telecom-ISAC Japan, and private-sector businesses.**
"Operation to Disable a Net Banking Virus" (http://www.keishicho.metro.tokyo.jp/haiteku/haiteku/haiteku504.htm) (in Japanese).

S **14th: INTERPOL announced they had taken down the SIMDA botnet together with investigative organizations and private-sector companies in various countries.**
This operation was carried out on April 9 and coordinated by the INTERPOL Global Complex for Innovation (IGCI), which INTERPOL established in Singapore to conduct research and development as well as investigative support regarding cybercrime countermeasures.
"INTERPOL coordinates global operation to take down Simda botnet" (http://www.interpol.int/News-and-media/News/2015/N2015-038).

S **14th: An incident occurred in which the domains of well-known companies such as Google and Yahoo were hijacked due to unauthorized access to Malaysian .my domains by an unknown attacker.**
MYNIC, "GOOGLE & YAHOO MALAYSIA DOMAIN BACK TO NORMAL WITHIN 24 HOURS"
(https://www.mynic.my/upload_media/press_release.pdf).

V **15th: Microsoft published their Security Bulletin Summary for April 2015, and released 11 updates, including four critical updates such as MS15-034, as well as seven important updates.**
"Microsoft Security Bulletin Summary for April 2015" (https://technet.microsoft.com/library/security/ms15-apr).

V **15th: A number of vulnerabilities in Adobe Flash Player that could allow arbitrary code execution were discovered and fixed.**
"Security updates available for Adobe Flash Player" (http://helpx.adobe.com/security/products/flash-player/apsb15-06.html).

V **15th: Oracle released their quarterly scheduled update for a number of products including Oracle, fixing a total of 98 vulnerabilities, including 14 in Java SE. Support for Java 7 ended as of this update.**
"Oracle Critical Patch Update Advisory - April 2015" (http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html).

O **15th: The European Commission (EC) announced they had send a Statement of Objections to Google, due to suspicions Google had violated EU antitrust laws by abusing their dominant position as a search service to give their own shopping service preferential treatment in general search results. The commission also stated they would investigate the Android mobile operating system separately.**
See the following press release for more information, "Antitrust: Commission sends Statement of Objections to Google on comparison shopping service" (http://europa.eu/rapid/press-release_MEMO-15-4781_en.htm).
For information on the Android mobile operating system, see "Antitrust: Commission opens formal investigation against Google in relation to Android mobile operating system" (http://europa.eu/rapid/press-release_MEMO-15-4782_en.htm).

V **22nd: A number of vulnerabilities in WordPress, including an XSS vulnerability that could allow arbitrary code execution by unauthorized users, were discovered and fixed.**
"WordPress 4.1.2 Security Release" (https://wordpress.org/news/2015/04/wordpress-4-1-2/).

V **28th: An XSS vulnerability in WordPress that could allow arbitrary code execution on a server via comment posting was discovered and fixed.**
"WordPress 4.2.1 Security Release" (https://wordpress.org/news/2015/04/wordpress-4-2-1/).

*Dates are in Japan Standard Time

Legend V Vulnerabilities | S Security Incidents | P Political and Social Situation | H History | O Other

In May, a buffer overflow vulnerability (CVE-2015-3456) in QEMU's virtual Floppy Disk Controller was disclosed by U.S. security firm CrowdStrike and fixed. This vulnerability was named VIRTUALIZED ENVIRONMENT NEGLECTED OPERATIONS MANIPULATION (VENOM) by the discoverer. Its impact was widespread, and it garnered a lot of attention because it allowed DoS attacks and arbitrary code execution on a host from the guest side in virtualization software such as Xen or KVM, which are used for cloud services.

Also in May, a vulnerability in the TLS protocol DH key exchange (CVE-2015-4000) that could allow an attacker to intercept or alter communications by forcing a downgrade to a weaker cipher via a MITM attack was discovered and fixed. This vulnerability was given the name Logjam, and like the FREAK vulnerability in SSL/TLS disclosed in March, it generated a lot of news due to its potential to affect many servers and browsers.

■ Malware Infections and Information Leaks Due to Targeted Attacks

During the current survey period, there were frequent incidents such as malware infections on PCs within organizations, as well as resulting information leaks. In June, the personal information of 1,010,000 people was leaked due to infection by malware attached to emails at the Japan Pension Service*14. Due to this incident, it was later revealed that similar incidents had been occurring since September last year at a number of companies and organizations, as well as hospitals and universities. In each case, it is known the infection took place via so-called targeted emails that had malware attached, with the sender misrepresented using free email accounts. Upon infection, the malware sent files on the infected PC or shared servers to an external party.

Similarly, there have also been reports of malware infections through email that was misrepresented as being from a multi-function printer*15. Other than these cases, malware infections on internal PCs and resulting information leaks have also occurred at a number of local public bodies. It has been identified that these infections may have been caused by so-called watering hole attacks, when users accessed an altered website.

In May, the IPA published the "Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP) Annual Activity Report FY2014," which summarized the activities of the Cyber Security Information sharing Partnership of Japan (J-CSIP)*16. In this report, it was mentioned that ongoing attacks thought to have been carried out by the same attacker have been observed over the course of 31 months. As these facts demonstrate, attacks are becoming more diverse through the appearance of new techniques and methods, and the increasing sophistication of the malware used. It is becoming difficult to deal with these threats using a stand-alone countermeasure, such as the introduction of anti-virus software. Efforts are underway to examine countermeasures for attacks like this that cannot be handled using existing security measures. One example is the "System Design Guide for Thwarting Advanced Targeted Email Attacks"*17 published by the IPA in September 2014.

■ Information Leaks Due to Unauthorized Access

Information leaks caused by unauthorized access also continue to occur. In May, the website of a U.S. beauty-related company was accessed without authorization, leading to the leak of credit card information and other data. The internal database of a U.S. insurance company was also compromised, causing the leak of personal information for 1.1 million individuals. In June, data related to approximately 100,000 taxpayers leaked from the U.S. Internal Revenue Service (IRS). The U.S. Office of Personnel Management was also accessed without authorization, and data on roughly 4 million federal employees leaked. Also in June, a U.S. password management service was compromised, and users were prompted to change their master password due to the possibility that some authentication information had leaked.

*14 Japan Pension Service, "An apology to Japan Pension Service customers whose personal information was leaked" (http://www.nenkin.go.jp/n/data/service/0000028648uArRENS1eQ.pdf) (in Japanese).

*15 Emails misrepresented as being from a multi-function printer have been known for a long time, but Trend Micro's security blog reported that these incidents spiked sharply in June.
"Japan also affected by emails misrepresented as notifications from multi-function printers that distribute macro-type malware" (http://blog.trendmicro.co.jp/archives/11776) (in Japanese).

*16 An initiative established in 2011 for carrying out early responses and information sharing between member organizations, with a focus on critical infrastructure companies. "Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP)" (https://www.ipa.go.jp/security/J-CSIP/) (in Japanese).

*17 IPA, "System Design Guide for Thwarting Advanced Targeted Email Attacks" (http://www.ipa.go.jp/files/000035723.pdf).

May Incidents

1

V **7th: A number of vulnerabilities in WordPress, including an XSS vulnerability that could allow arbitrary code execution by unauthorized users, were discovered and fixed.**
"WordPress 4.2.2 Security and Maintenance Release" (https://wordpress.org/news/2015/05/wordpress-4-2-2/).

2

3

O **12th: IPA published their SSL/TLS encryption configuration guidelines, to enable encryption settings that take into consideration appropriate security for SSL/TLS server builders and operators.**
"SSL/TLS Encryption Configuration Guidelines - For a Secure Website (Encryption Configuration Measures)" (http://www.ipa.go.jp/security/vuln/ssl_crypt_config.html) (in Japanese).

4

5

V **13th: Microsoft published their Security Bulletin Summary for May 2015, and released 13 updates, including three critical updates, MS15-043, MS15-044 and MS15-45, as well as 10 important updates.**
"Microsoft Security Bulletin Summary for May 2015" (https://technet.microsoft.com/library/security/ms15-may).

6

V **13th: A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination or arbitrary code execution were discovered and fixed.**
"APSB15-09: Security updates available for Adobe Flash Player" (https://helpx.adobe.com/security/products/flash-player/apsb15-09.html).

7

8

9

10

V **14th: A vulnerability (CVE-2015-3456) in the QEMU Floppy Disk Controller (FDC) used in Xen and KVM that could allow abnormal server termination or arbitrary code execution was discovered and fixed. This vulnerability was named VENOM by the discoverer.**
See the following website of the discoverer, CrowdStrike, for more information. "VENOM VIRTUALIZED ENVIRONMENT NEGLECTED OPERATIONS MANIPULATION" (http://venom.crowdstrike.com/).

11

O **15th: IETF published HTTP/2, which was approved in February, as an RFC.**
"Hypertext Transfer Protocol Version 2 (HTTP/2)" (http://www.rfc-editor.org/rfc/rfc7540.txt).

12

13

V **21st: A vulnerability in the TLS protocol DH key exchange that could allow communications to be intercepted or altered by forcing selection of weaker encryption through a MITM attack was discovered and fixed.**
See the following explanation by the discoverer for more details. "The Logjam Attack" (https://weakdh.org/).

14

S **22nd: DDoS attacks accompanied by threats were made on a number of financial institutions and online stores, resulting in systems being difficult to access, etc.**

15

O **22nd: The Ministry of Internal Affairs and Communications published its Recommendations on Promotion of Cyber Security Policy coordinated by the Information Security Advisory Board.**
"'Recommendations on Promotion of Cyber Security Policy' published" (http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000093.html) (in Japanese).

16

17

O **22nd: IPA and JPCERT/CC published the 2015 version of the "Information Security Early Warning Partnership Guidelines," for reference when reporting or receiving notification of information related to vulnerabilities. This relates to the Information Security Early Warning Partnership, an initiative for promoting the trouble-free distribution of vulnerability information and the spread of countermeasures.**
IPA, "Information Security Early Warning Partnership Guidelines" (http://www.ipa.go.jp/security/ciadr/partnership_guide.html) (in Japanese).

18

19

S **25th: The National Police Agency issued an alert regarding an increase in scanning activity that targets a utility tool for an online game.**
This tool has a proxy function implemented, so this scanning activity is thought to be searching for so-called open proxies that can be used externally by a third party. See "Regarding an increase in proxy searches targeting specific ports" (http://www.npa.go.jp/cyberpolice/detect/pdf/20150525.pdf) (in Japanese) for more information.

20

21

O **25th: The 2nd general meeting of the Cyber Security Strategic Headquarters was held, and a new Cyber Security Strategy (proposed) that determines the basic policy for cyber security measures was decided on.**
NISC, "Cybersecurity Strategy" (http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf).

22

23

S **26th: The National Police Agency issued an alert regarding an increase in scanning activity targeting vulnerabilities in certain PLC software used in industrial control systems.**
"Regarding the observation of access targeting vulnerabilities in the PLC used in industrial control systems" (http://www.npa.go.jp/cyberpolice/detect/pdf/20150526.pdf) (in Japanese).

24

25

S **26th: The JPCERT Coordination Center issued an alert regarding the alteration of website content and resulting occurrence of ransomware infections through redirection to attack sites.**
"Alert regarding ransomware infections" (https://www.jpcert.or.jp/english/at/2015/at150015.txt).

26

27

S **27th: The U.S. Internal Revenue Service (IRS) was accessed without authorization, and information such as the social security numbers of around 100,000 taxpayers leaked.**
"IRS Statement on the 'Get Transcript' Application" (http://www.irs.gov/uac/Newsroom/IRS-Statement-on-the-Get-Transcript-Application).

28

29

30

31

*Dates are in Japan Standard Time

Legend

V Vulnerabilities | S Security Incidents | P Political and Social Situation | H History | O Other

In Japan, there were also incidents of unauthorized access at one of the major ISPs in May, leading to the leak of FTP accounts, etc. In April, there was an incident in which internal documents from a university were published on the Internet due to flawed server configuration. In June, a server for operation verification used at the National Institute of Informatics was accessed without authorization and exploited as a stepping stone in a DDoS attack, due to a weak password being configured. In an incident in which registered information leaked from a stockholders service site, unauthorized access from outside was suspected in April when the leak was disclosed, but the final report published in May revealed that it was an inside job.

■ Government Agency Initiatives

Government agency activities with regard to security measures included the holding of the 2nd general meeting of the Cyber Security Strategic Headquarters in May, where a new Cyber Security Strategy (proposed) that determines basic policy for cyber security measures was decided on. This set forth cyber security policy for around the next three years, laying out a course of action for items such as the promotion of research and development and cultivation of human resources to meet objectives, in light of the 2020 Olympic and Paralympic Games to be held in Tokyo. It is next scheduled to undergo revisions through public comment, before a cabinet decision is made.

In April, a proposal was put together for revisions to the Guidelines for the Protection of Personal Information in the Telecommunications Business and Explanation, which were under consideration by the "Working Group on the Handling of Personal and User Information" held under the supervision of the Ministry of Internal Affairs and Communications' ICT Service Safety and Security Study Group. Following amendments based on public comment, the proposed revisions were made in June. The main revised points included the addition of specific examples for the appropriate acquisition of personal information, guidelines for the retention period for connection authentication logs with regards to communication history, and the deletion of conditions for acquiring location information during a criminal investigation.

■ Other

In April, the INTERPOL Global Complex for Innovation (IGCI), an organization specializing in cybercrime countermeasures that the International Criminal Police Organization (ICPO) established in Singapore, began full operation*18. Ahead of this, the IGCI coordinated a takedown of the Simda botnet in collaboration with law enforcement agencies and private-sector businesses in various countries. In Japan, the Tokyo Metropolitan Police Department, the Ministry of Internal Affairs and Communications, Telecom-ISAC Japan, and private-sector companies worked together in the VAWTRAK takedown operation.

In May, it was discovered that the SourceForge open source software library site had bundled and distributed third-party software in software installers published on the site without permission. This resulted in them receiving complaints from the development project*19, and massive backlash from other developers and the community. Due to the overwhelmingly negative reaction they received, SourceForge has rescinded this policy*20.

Additionally, between May and June there were DDoS attacks accompanied by threats that targeted a number of financial institutions and online stores. In these attacks, the threats included demands for payment via bitcoin, with the implication that a DDoS attack of several hundred Gbps would be made if these demands were not met. The DDoS attacks and payment via bitcoin are points similar to attacks made since last year by a group calling themselves DD4BC, so it is thought they may be involved*21. Attacks have also been made on financial institutions in Europe and Hong Kong, so ongoing vigilance is required.

In June, a minor was arrested on suspicion of involvement in an incident that occurred in December 2014 in which the website of a publisher was accessed without authorization, and altered to redirect visitors to another website. This minor was arrested again in July on suspicion of using someone else's credit card without permission.

*18 "International gathering marks inauguration of INTERPOL Global Complex for Innovation" (http://www.interpol.int/News-and-media/News/2015/N2015-039).
*19 GIMP PROJECT, "GIMP PROJECT'S OFFICIAL STATEMENT ON SOURCEFORGE'S ACTIONS" (http://www.gimp.org/).
*20 SourceForge Community Blog, "Third party offers will be presented with Opt-In projects only" (http://sourceforge.net/blog/third-party-offers-willbe-presented-with-opt-in-projects-only/).
*21 See the following Arbor Networks report for more information on DD4BC. "DD4BC DDoS Extortion Threat Activity" (https://asert.arbornetworks.com/dd4bc-ddos-extortion-threat-activity/).

June Incidents

S 1st: The Japan Pension Service announced that the personal information of up to 1.25 million people may have leaked after it was accessed without authorization due to a malware infection.
"Regarding the leak of personal information from the Japan Pension Service"
(http://www.nenkin.go.jp/oshirase/topics/2015/20150721.files/0000150601ndjlleouli.pdf) (in Japanese).

O 3rd: The USA Freedom Act, which includes provisions that reform the monitoring activities of the National Security Agency (NSA), was passed in the U.S. Senate, and signed into law by the President. This law limits the information gathering activities of the NSA, which had been criticized for its mass collection of phone records around the world, including those of U.S. citizens.
Congress.gov, "H.R.2048 - USA FREEDOM Act of 2015" (https://www.congress.gov/bill/114th-congress/house-bill/2048/text).

S 5th: The U.S. Office of Personnel Management (OPM) was accessed without authorization, and data on roughly 4 million federal employees leaked.
"OPM to Notify Employees of Cybersecurity Incident"
(https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/).

S 5th: The National Institute of Informatics announced that one of its servers for operation verification had been accessed without authorization, and used as a stepping stone in a DoS attack.
"Unauthorized access on operation verification server" (http://www.nii.ac.jp/news/2015/0605) (in Japanese).

O 5th: A newly-merged company issued an alert after a domain it had used previously was obtained by a third party, and used to redirect users to other sites, including fraudulent ones.

V 10th: Microsoft published their Security Bulletin Summary for June 2015, and released eight updates, including two critical updates MS15-056 and MS15-57, as well as six important updates.
"Microsoft Security Bulletin Summary for June 2015" (https://technet.microsoft.com/library/security/ms15-jun).

V 10th: A number of vulnerabilities in Adobe Reader and Acrobat that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB15-10: Security updates available for Adobe Reader and Acrobat" (https://helpx.adobe.com/security/products/reader/apsb15-10.html).

O 12th: The Ministry of Internal Affairs and Communications issued an alert due to incidents in which telephone services such as IP phones were used by third parties without authorization, resulting in users being billed for expensive international telephone charges.
Causes included the exploitation of vulnerabilities in PBX or routers connected to IP phones, and the theft of IDs and passwords for use in international phone calls due to a weak password being assigned. "Alert regarding the unauthorized use of IP phones by third parties"
(http://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000191.html) (in Japanese).

S 16th: U.S. company LastPass, which provides a password management tool, announced it had been compromised and some authentication hashes and user account information had leaked.
"LastPass Security Notice" (https://blog.lastpass.com/2015/06/lastpass-security-notice.html/).

O 16th: The Council of Anti-Phishing Japan issued an alert due to confirmation of techniques redirecting users to a banking phishing site using SMS (Short Message Service) at a number of banks from late May.
"[Alert] Beware of redirection to bank phishing sites by SMS (Short Message Service) (June 16, 2015)"
(https://www.antiphishing.jp/news/alert/_sms_20150616.html) (in Japanese).

V 17th: A number of vulnerabilities that could allow arbitrary code execution were discovered and fixed in the keyboard function of the SwiftKey SDK used in Samsung brand mobile devices.
US-CERT, "Vulnerability Note VU#155412 Samsung Galaxy S phones fail to properly validate SwiftKey language pack updates"
(http://www.kb.cert.org/vuls/id/155412).

S 22nd: The flight plan computers of LOT Polish Airlines were attacked, causing flights to be canceled or delayed.
LOT Polish Airlines, "TODAY AFTERNOON LOT ENCOUNTERED IT ATTACK, THAT AFFECTED OUR GROUND OPERATION SYSTEMS."
(http://corporate.lot.com/pl/en/press-news?article=772922).

V 24th: A vulnerability in Adobe Flash Player that could allow arbitrary code execution was discovered and fixed. It was confirmed that this vulnerability had already been exploited in limited targeted attacks.
"Security updates available for Adobe Flash Player" (https://helpx.adobe.com/security/products/flash-player/apsb15-14.html).

O 24th: The Ministry of Internal Affairs and Communications revised its Guidelines for the Protection of Personal Information in the Telecommunications Business and Explanation.
"Guidelines for the Protection of Personal Information in the Telecommunications Business"
(http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/telecom_perinfo_guideline_intro.html) (in Japanese).

S 25th: DDoS attacks accompanied by threats were made on the online systems of a certain bank, resulting in systems being difficult to access, etc.

*Dates are in Japan Standard Time

Legend V Vulnerabilities | S Security Incidents | P Political and Social Situation | H History | O Other

The Ministry of Internal Affairs and Communications issued an alert due to a rise in the number of incidents in which telephone services such as IP phones were used by a third party without authorization, resulting in users being billed for expensive international telephone charges. Subsequently, a security firm pointed out that the products of a certain vendor had caused significant damages because they were operated with a default password set, and allowed access from the Internet, but the vendor has denied this. Regarding this issue, based on discussions at the Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business, in July the Ministry of Internal Affairs and Communications sent a request for cooperation to telecommunications business organizations, asking them to make it known that telecommunications companies that have contracts with users to provide international telephone services should take appropriate measures to stop unauthorized use before it occurs, and prevent the spread of damages*22.

A series of several vulnerabilities were discovered on SSL/TLS servers. Meanwhile, there are also issues such as the fact that applying the latest countermeasures prevents connection from older devices, meaning that designs and operation that account for the tradeoff between security and required compatibility are necessary. In answer to this, in May the IPA published their SSL/TLS encryption configuration guidelines, to enable encryption settings that take into consideration appropriate security for SSL/TLS server builders and operators.

1.3 Incident Survey

1.3.1 DDoS Attacks

Today, DDoS attacks on corporate servers are almost a daily occurrence, and the methods involved vary widely. However, most of these attacks are not the type that utilizes advanced knowledge such as that of vulnerabilities, but rather cause large volumes of unnecessary traffic to overwhelm network bandwidth or server processes for the purpose of hindering services.

■ Direct Observations

Figure 2 shows the circumstances of DDoS attacks handled by the IIJ DDoS Protection Service between April 1 and June 30, 2015.

This information shows traffic anomalies judged to be attacks based on IIJ DDoS Protection Service standards. IIJ also responds to other DDoS attacks, but these incidents are excluded from the figure due to the difficulty in accurately ascertaining the facts of each situation.

There are many methods that can be used to carry out a DDoS attack, and the capacity of the environment attacked (bandwidth and server performance) will largely determine the degree of impact. Figure 2 categorizes DDoS attacks into three types: attacks

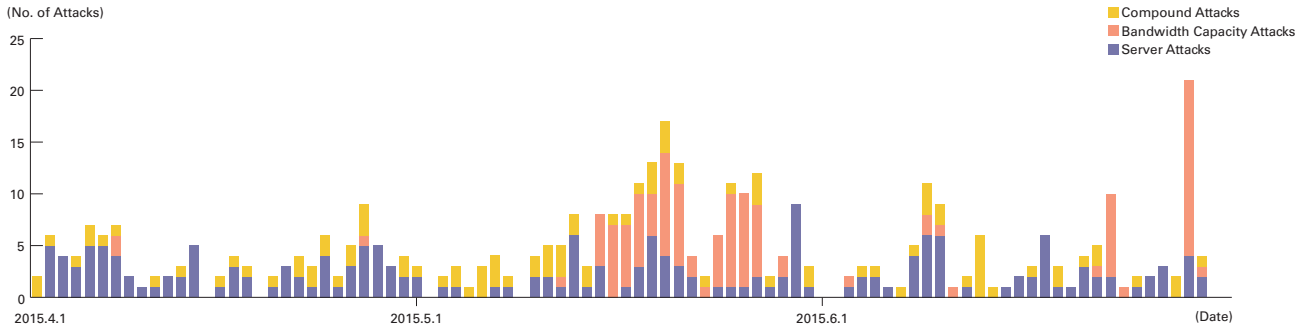


Figure 2: Trends in DDoS Attacks

*22 Ministry of Internal Affairs and Communications, "Regarding measures to prevent the unauthorized use of IP phones, etc., by third parties (request)" (http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000096.html) (in Japanese).

on bandwidth capacity*23, attacks on servers*24, and compound attacks (several types of attacks on a single target conducted at the same time).

During the three months under study, IIJ dealt with 361 DDoS attacks. This averages to 3.97 attacks per day, indicating a decrease in the average daily number of attacks compared to our prior report. Server attacks accounted for 52.1% of all incidents, while compound attacks accounted for 14.9%, and bandwidth capacity attacks 33%. The largest attack observed during the period under study was classified as a compound attack, and resulted in 8.25 Gbps of bandwidth using up to 2,713,000 pps packets.

Of all attacks, 77.3% ended within 30 minutes of commencement, 22.7% lasted between 30 minutes and 24 hours, and none lasted over 24 hours. The longest sustained attack was a compound attack that lasted for 10 hours and 37 minutes.

In most cases, we observed an extremely large number of IP addresses, whether domestic or foreign. We believe this is accounted for by the use of IP spoofing*25 and botnet*26 usage as the method for conducting DDoS attacks.

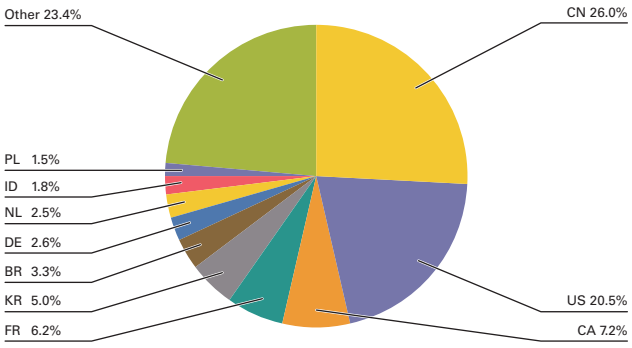


Figure 3: DDoS Attack Targets by Country According to Backscatter Observations

■ Backscatter Observations

Next we present our observations of DDoS attack backscatter using the honeypots*27 set up by the MITF, a malware activity observation project operated by IIJ*28. By monitoring backscatter it is possible to detect some of the DDoS attacks occurring on external networks as a third party without any interposition.

For the backscatter observed between April 1 and June 30, 2015, Figure 3 shows the sender's IP addresses classified by country, and Figure 4 shows trends in packet numbers by port.

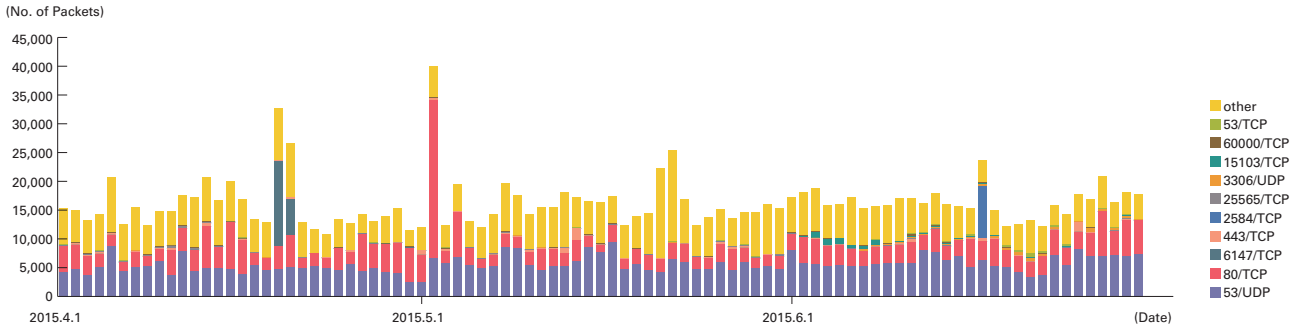


Figure 4: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)

*23 Attack that overwhelms the network bandwidth capacity of a target by sending massive volumes of larger-than-necessary IP packets and fragments. The use of UDP packets is called a UDP flood, while the use of ICMP packets is called an ICMP flood.

*24 TCP SYN flood, TCP connection flood, and HTTP GET flood attacks. TCP SYN flood attacks send mass volumes of SYN packets that signal the start of TCP connections, forcing the target to prepare for major incoming connections, causing the wastage of processing capacity and memory. TCP connection flood attacks establish mass volumes of actual TCP connections. HTTP GET flood attacks establish TCP connections on a Web server, and then send mass volumes of HTTP GET protocol commands, wasting processing capacity and memory.

*25 Misrepresentation of a sender's IP address. Creates and sends an attack packet that has been given an address other than the actual IP address of the attacker to make it appear as if the attack is coming from a different location, or from a large number of individuals.

*26 A "bot" is a type of malware that institutes an attack after receiving a command from an external C&C server. A network constructed of a large number of bots acting in concert is called a botnet.

*27 Honeypots established by the MITF, a malware activity observation project operated by IIJ. See also "1.3.2 Malware Activities."

*28 The mechanism and limitations of this observation method, as well as some of the results of IIJ's observations, are presented in Vol.8 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol08_EN.pdf) under "1.4.2 Observations on Backscatter Caused by DDoS Attacks."

The port most commonly targeted by the DDoS attacks observed was the 53/UDP port used for DNS, accounting for 34.5% of the total. This was followed by 80/TCP used for Web services at 22.3%, so the top two ports accounted for 56.8% of the total. Attacks were also observed on 443/TCP used for HTTPS, 53/TCP used for DNS, and 25565/TCP sometimes used for game servers, as well as 6147/TCP and 2584/TCP, which are not commonly used.

Examining the daily average number of packets for the 53/UDP communications observed often since February 2014, we can see that although it dropped from around 6,200 in the previous survey period to around 5,600, it remains high.

Looking at the origin of backscatter thought to indicate IP addresses targeted by DDoS by country in Figure 3, China accounted for the largest ratio at 26.0%. The United States and Canada followed at 20.5% and 7.2%, respectively.

Regarding particularly large numbers of backscatter packets observed by port, there were attacks on the Web servers (80/ TCP) of a U.S. hosting provider between April 26 and May 1, and on the server group of a hosting provider in Canada on May 2. Attacks observed on other ports included those targeting 6147/TCP between April 19 and 20, but because the source IP address for the backscatter was a private address, the attack target is not known. On June 17, attacks on the servers of a U.S. ISP that targeted 2584/TCP were observed.

Notable DDoS attacks during the current survey period that were detected via IIJ's observations of backscatter included attacks on a U.K. online casino between April 13 and April 15, and attacks on a French company involved in nuclear energy May 5. Attacks were also detected on a number of government agency sites in Canada on June 18 and June 28.

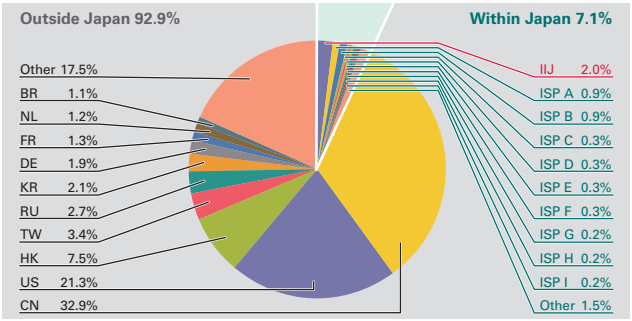


Figure 5: Sender Distribution (by Country, Entire Period under Study)

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the MITF*29, a malware activity observation project operated by IIJ. The MITF uses honeypots*30 connected to the Internet in a manner similar to general users in order to observe communications arriving over the Internet. Most appear to be communications by malware selecting a target at random, or scans attempting to locate a target for attack.

■ Status of Random Communications

Figure 5 shows the distribution of sender's IP addresses by country for communications coming into the honeypots

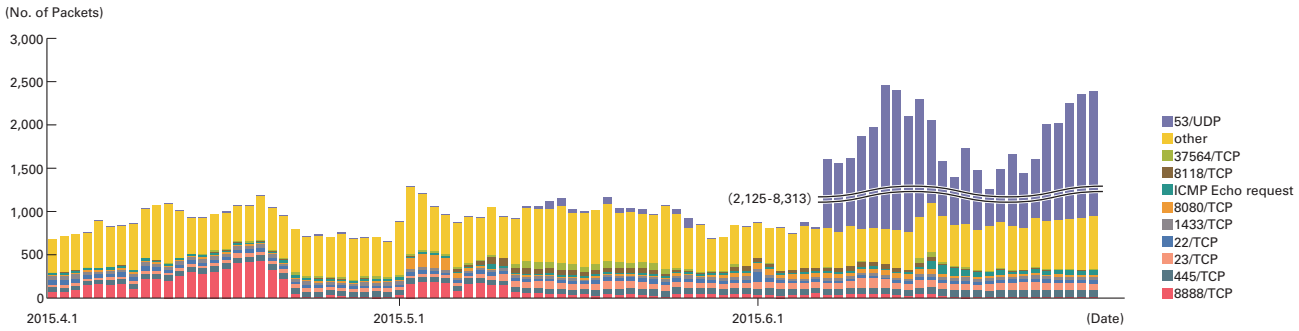


Figure 6: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

*29 An abbreviation of Malware Investigation Task Force. The Malware Investigation Task Force (MITF) began activities in May 2007, observing malware network activity through the use of honeypots in an attempt to understand the state of malware activities, to gather technical information for countermeasures, and to link these findings to actual countermeasures.

*30 A system designed to simulate damages from attacks by emulating vulnerabilities, recording the behavior of attackers, and the activities of malware.

between April 1 and June 30, 2015. Figure 6 shows trends in the total volumes (incoming packets). The MITF has set up numerous honeypots for the purpose of observation. We have taken the average per honeypot, showing the trends for incoming packet types (top ten) over the entire period subject to study. Additionally, in these observations we corrected data to count multiple TCP connections as a single attack when the attack involved multiple connections to a specific port, such as attacks on MSRPC.

Much of the communications arriving at the honeypots during the current survey period were DNS Water Torture attack attempts, communications searching for devices to carry out DoS attacks on by amplifying response packets, communications searching for proxy servers, or scanning behavior targeting TCP ports used by Microsoft operating systems. Between June 7 and June 30, a large volume of communications targeting 53/UDP, used by DNS servers, occurred on one of our honeypots. Although the source IP address distribution for these communications was centered on the United States and China, they were mostly unique and covered a wide range, so it is possible that either a bot was used, or the source addresses were spoofed. Upon investigating the content of these communications, we found they were repeated queries for A records that do not exist, such as "(random string). www.example.com." For this reason, we believe this was an example of DNS Water Torture*31. Several of the domains targeted in these attacks were servers in China (.com domains).

From a number of IP addresses, we also observed scanning behavior for 5353/UDP used for multicast DNS, 123/UDP used for NTP, and 5351/UDP used for NAT-PMP along with DNS TXT record queries. We believe these were searches for devices that could be used in reflection attacks by sending packets spoofed to be from the site you want to attack, amplifying the response packets. With regard to the 5351/UDP communications, there have been reports*32 claiming it was possible to control NAT-PMP externally on some devices, so this could have been a search for vulnerable devices.

From April to early May, there was an increase in 8888/TCP communications. These communications were carried out repeatedly, targeting a wide range of IP addresses from two IP addresses allocated to China. At the same time as 8888/TCP, scanning behavior was also observed for ports such as 37564/TCP*33 used by the KanColleViewer utility tool for an online game, 8118/TCP*34 used by a proxy server called Privoxy, 3128/TCP that is set by default for a number of proxy servers such as Squid, and 8090/TCP used as a backup for 8123/TCP and 8080/TCP, which are used by a proxy server called Polipo. For this reason, we believe these communications were searches for open proxy servers.

■ Malware Network Activity

Figure 7 shows the distribution of the specimen acquisition source for malware during the period under study, while Figure 8 shows trends in the total number of malware specimens acquired. Figure 9 shows trends in the number of unique specimens. In Figure 8 and Figure 9, the number of acquired specimens show the total number of specimens acquired per day*35, while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*36. Specimens are also identified using anti-virus software, and a breakdown of the top 10 variants is displayed color coded by malware name. As

*31 Secure64 Software Corporation, "Water Torture: A Slow Drip DNS DDoS Attack" (https://blog.secure64.com/?p=377). For an explanation in Japanese, see the following document written by Mr. Yasuhiro Orange Morishita of Japan Registry Services. "DNS Water Torture Attacks" (http://2014.seccon.jp/dns/dns_water_torture.pdf) (in Japanese). The MITF honeypots do not query authoritative servers or cache servers when they receive DNS query packets, so they provide no aid to attacks.

*32 "Vulnerability Note VU#184540 Incorrect implementation of NAT-PMP in multiple devices" (http://www.kb.cert.org/vuls/id/184540). Scanning behavior targeting this port has also been reported in the past. "Regarding scanning behavior for devices that allow external control of NAT-PMP" (http://www.npa.go.jp/cyberpolice/detect/pdf/20141030.pdf) (in Japanese).

*33 Because the KanColleViewer was configured as an open proxy by default, JVN and others issued an alert. "VNVU#98282440 Issues with 'Teitoku Gyo Mo Isogashii!' (KanColleViewer) operating as an open proxy" (https://jvn.jp/vu/JVNVU98282440/) (in Japanese). The National Police Agency also reported an increase in scanning for this port. "Regarding an increase in proxy searches targeting specific ports" (http://www.npa.go.jp/cyberpolice/detect/pdf/20150525.pdf) (in Japanese).

*34 An increase in access targeting this port has been reported in the past. "Internet observation results, etc. (January 2015)" (https://www.npa.go.jp/cyberpolice/detect/pdf/20150304.pdf) (in Japanese).

*35 This indicates the malware acquired by honeypots.

*36 This figure is derived by utilizing a one-way function (hash function) that outputs a fixed-length value for various input. The hash function is designed to produce as many different outputs as possible for different inputs. While we cannot guarantee the uniqueness of specimens by hash value, given that obfuscation and padding may result in specimens of the same malware having different hash values, the MITF has expended its best efforts to take this fact into consideration when using this methodology as a measurement index.

with our previous report, for Figure 8 and Figure 9 we have detected Conficker using multiple anti-virus software packages, and removed any Conficker results when totaling data.

On average, 91 specimens were acquired per day during the period under study, representing 17 different malware. After investigating the undetected specimens more closely, they included worms observed from IP addresses allocated to countries such as China, the United States, India, Taiwan, and Austria. Additionally, about 55% of undetected specimens were in text format. Because many of these text format specimens were HTML 404 or 403 error responses from Web servers, we believe this was due to infection behavior of malware such as old worms continuing despite the closure of download sites that newly-infected PCs access to download malware.

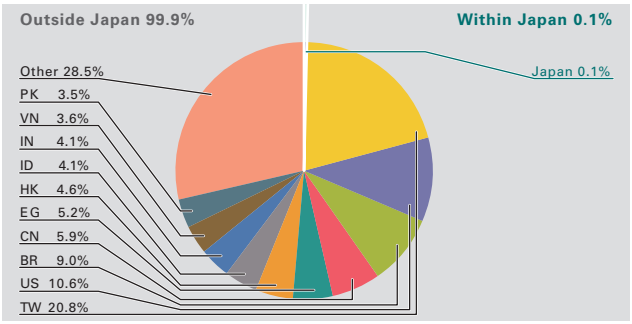


Figure 7: Distribution of Acquired Specimens by Source (by Country, Entire Period under Study, Excluding Conficker)

Under the MITF's independent analysis, during the current period under observation 90.0% of malware specimens acquired were worms, 1.8% were bots, and 8.2% were downloaders. In addition, the MITF confirmed the presence of 106 botnet C&C servers*37 and 9 malware distribution sites. The number of botnet C&C servers is higher than before, but this was due to the appearance of a specimen that used a DGA (Domain Generation Algorithm) during the current survey period.

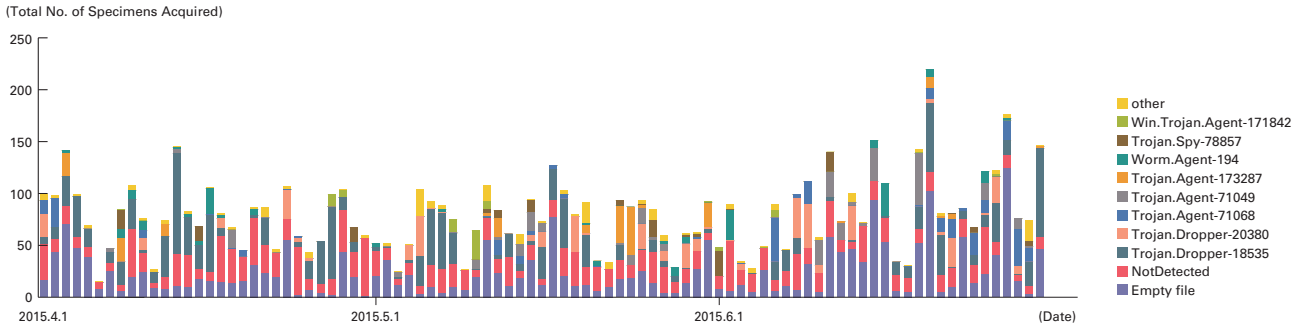


Figure 8: Trends in the Total Number of Malware Specimens Acquired (Excluding Conficker)

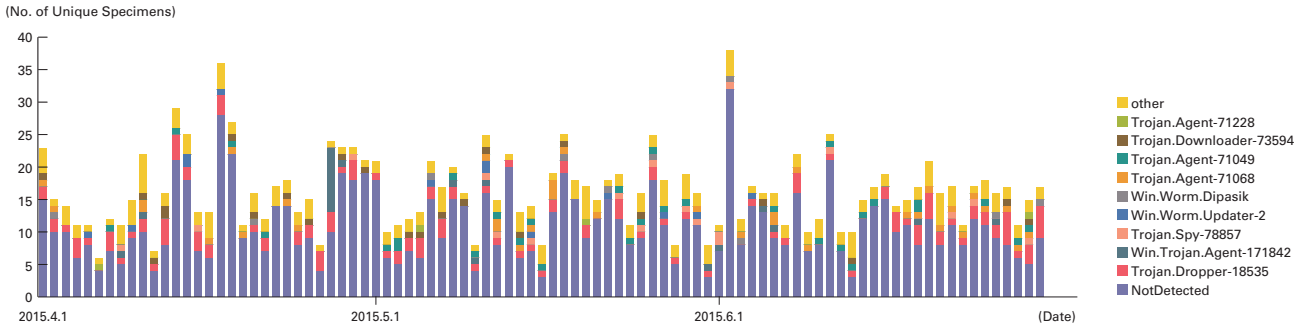


Figure 9: Trends in the Number of Unique Specimens (Excluding Conficker)

*37 An abbreviation of Command & Control Server. A server that provides commands to a botnet consisting of a large number of bots.

Conficker Activity

Including Conficker, an average of 27,999 specimens were acquired per day during the period covered by this report, representing 549 different malware. While figures rise and fall over short periods, Conficker accounts for 99.7% of the total number of specimens acquired, and 97.0% of unique specimens. This demonstrates that Conficker remains the most prevalent malware by far, so we have omitted it from figures in this report. Compared to the previous survey period, the total number of specimens acquired increased by approximately 44% during the period covered by this report, and the number of unique specimens decreased by about 10%. The increase in the total number of specimens acquired was due to a spike in infection activity from IP addresses allocated to the United States during the current survey period. According to the observations of the Conficker Working Group*38, as of July 1, 2015, a total of 775,060 unique IP addresses are infected. This indicates a drop to about 24% of the 3.2 million PCs observed in November 2011, but it demonstrates that infections are still widespread.

1.3.3 SQL Injection Attacks

Of the types of different Web server attacks, IIJ conducts ongoing surveys related to SQL injection attacks*39. SQL injection attacks have flared up in frequency numerous times in the past, remaining one of the major topics in the Internet security. SQL injections are known to occur in one of three attack patterns: those that attempt to steal data, those that attempt to overload database servers, and those that attempt to rewrite Web content.

Figure 10 shows the distribution of SQL injection attacks against Web servers detected between April 1 and June 30, 2015. Figure 11 shows trends in the numbers of attacks. These are a summary of attacks detected by signatures on the IIJ Managed IPS Service. China was the source for 63.3% of attacks observed, while Japan and the United States accounted for 20.7% and 7.6%, respectively, with other countries following in order. There was a significant decrease in the number of SQL injection attacks against Web servers compared to the previous report. This is due to a drop in the number of large-scale attacks from China, although attacks from China are still continue to occur, and account for a large percentage of the total.

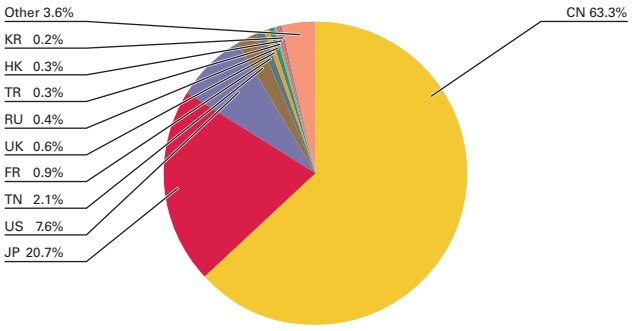


Figure 10: Distribution of SQL Injection Attacks by Source

During this period, attacks from a specific attack source in China directed at specific targets took place between April 22 and April 23. Attacks from a different specific attack source in China targeting specific targets occurred on May 14. On June 21, attacks were made from a number of sources in the United States and Europe directed at specific targets. These attacks are thought to have been attempts to find vulnerabilities on Web servers.

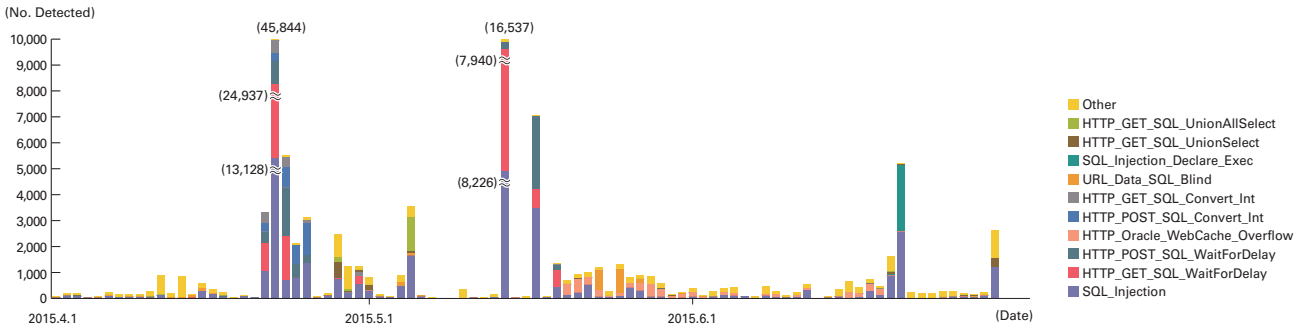


Figure 11: Trends in SQL Injection Attacks (by Day, by Attack Type)

*38 Conficker Working Group Observations (http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking).

*39 Attacks accessing a Web server to send SQL commands, thereby manipulating an underlying database. Attackers access or alter the database content without proper authorization, and steal sensitive information or rewrite Web content.

As previously shown, attacks of various types were properly detected and dealt with in the course of service. However, attack attempts continue, requiring ongoing attention.

1.3.4 Website Alterations

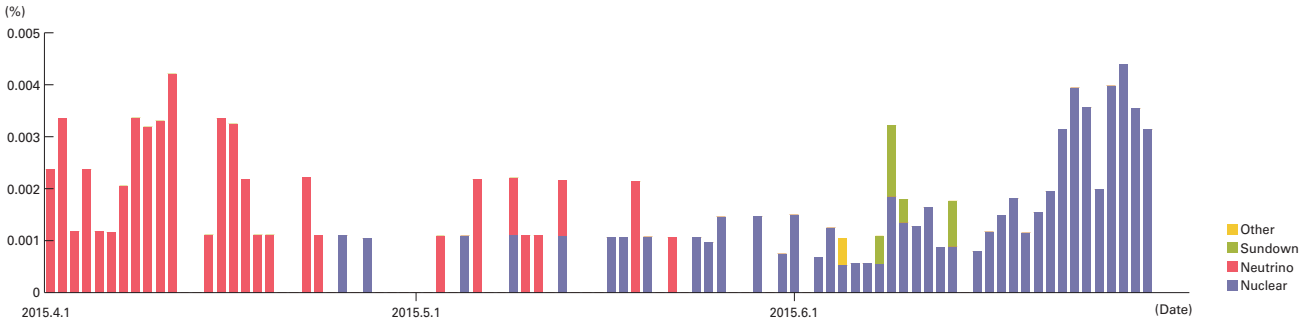
Here we indicate the status of website alterations as surveyed through the MITF Web crawler (client honeypot)*40.

This Web crawler accesses hundreds of thousands of websites on a daily basis, with a focus on well-known and popular sites in Japan. We also add new target sites on a regular basis. In addition to this, we temporarily monitor websites that have seen short-term increases in access numbers. By surveying websites thought to be viewed frequently by typical users in Japan, it is easier to speculate on trends regarding fluctuations in the number of altered sites, as well as the vulnerabilities exploited and malware distributed.

The number of drive-by download attacks observed between April 1 and June 30, 2015, was more than double the number seen between January 1 and March 31, 2015. In the first half of this survey period many cases of Neutrino were observed, while in the latter half most attacks had shifted to Nuclear (Figure 12). For a period of time in mid-June, A new exploit kit called Sundown was detected. Sundown is used in attacks targeting users in Japan in particular*41, and during observations by the MITF, we confirmed that the download of malware such as Kasidet ultimately took place, exploiting Flash vulnerabilities such as CVE-2015-0311 and CVE-2015-0313.

After updating the Web crawler system on July 1, 2015 to add functions and change the configuration, attacks were observed using Angler, which had not been detected by the MITF since January 2015. There were more Angler attacks than the total of other attacks combined, and since July 1 the total number of attacks detected has increased almost threefold. For this reason, we believe it highly likely that Angler was used in attacks targeting users in Japan before June 30 also. Also see "1.4.2 Angler Exploit Kit on the Rampage" for more information about our observations of Angler-based attacks and their details.

On the whole, attacks using drive-by downloads are occurring comparatively frequently. In early July 2015, a number of zero-day vulnerabilities that could be exploited by exploit kits were disclosed (CVE-2015-5119, CVE-2015-5122, etc.). Exploit kits such as the aforementioned Angler, Nuclear, and Neutrino added functions for exploiting these vulnerabilities in an extremely short period of time. We recommend browser users and administrators stay well aware of vulnerabilities in OSes and browser-related plug-ins, and carry out thorough countermeasures such as applying updates and enabling EMET. It is also important for website operators to implement countermeasures for Web content alteration and confirm the integrity of mashup content provided by third parties.



*Covers several hundreds of thousands of sites in Japan. In recent years, drive-by downloads have been configured to change attack details and whether or not attacks are made based on the client system environment or session information, source address attributes, and the quota achievement status of factors such as number of attacks. This means that results can vary wildly at times depending on the test environment and circumstances.

Figure 12: Rate of Drive-By Download Incidence When Viewing Websites (%) (by Exploit Kit)

*40 See "1.4.3 Website Defacement Surveys Using Web Crawlers" in Vol.22 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol22_EN.pdf) for an explanation of Web crawler observation methods.

*41 Regarding Sundown, "Fast look at Sundown EK" (http://malware.dontneedcoffee.com/2015/06/fast-look-at-sundown-ek.html) touches on its functions and attack targets based on information gained from the Control Panel, etc.

1.4 Focused Research

Incidents occurring over the Internet change in type and scope from one minute to the next. Accordingly, IIJ works toward implementing countermeasures by continuing to perform independent surveys and analyses of prevalent incidents. Here, we present information from the surveys we have undertaken during this period covering three themes. First, we discuss machine learning and security. Next, we look at the Angler Exploit Kit that has been spreading like wildfire. Finally, we examine the actual use of ID management technology.

1.4.1 Machine Learning and Security

Machine learning is a branch of artificial intelligence, which has been studied for many years. This field involves the research and development of algorithms that improve their output automatically based on known data, much like human beings learn from experience. Together with the accumulation of a large amount of data on the Internet, and the availability of vast computational resources at a reasonable price due to cloud computing, etc., the academic achievements of machine learning and its applications in IT systems are being discussed more often these days.

In the past, when there was a topic for which the decision-making criteria could be made explicit, efforts were made to automate it using programming. Machine learning techniques can be used to learn from and imitate human decision making, even with topics for which criteria cannot easily be made explicit, and this is expected to be useful for promoting automation.

In the field of security, automatic decision making has been carried out using explicit criteria such as blacklists, whitelists, and signatures, but it is hoped that machine learning techniques will be effective for the many instances in which decision making is not easy using these methods alone. Additionally, as the difficulty of training security staff and the burden of their daily decision-making work are now recognized as issues, machine learning has attracted attention as a technology for automating or supporting decision-making tasks.

In this report, we give a broad overview of machine learning and examples of its application in the field of security, then examine whether it can be applied as a countermeasure to a number of threat types. We also consider the security risks of systems that incorporate machine learning.

■ About Machine Learning

First, we will discuss the main machine learning systems (Figure 13). When using machine learning, you first prepare training data consisting of pairs of input and expected output in advance*42. Human decision making is "learned" beforehand using this training data, then an algorithm for decision making and the learned results are built in to the system you want to carry out automatic decision making on.

Decision-making algorithms generally incorporate many internal parameters, and are designed so that output changes in various ways according to the values set. The aforementioned "learning" is essentially the calculation of the appropriate setting values to comply with the training data. A range of techniques are being developed and researched using a decision making algorithm and the "learning algorithm" procedure for calculating its set values, such as neural networks, support vector machines (SVM), and decision tree learning.

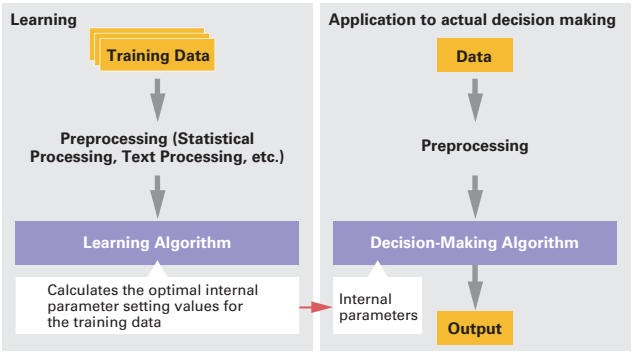


Figure 13: Supervised Machine Learning

When applying this to actual topics, it is necessary to analyze the topic in question and its data, select a suitable machine learning algorithm, and implement preprocessing (statistical processing, text processing, etc.) of input so it is easier for that algorithm to learn and make decisions.

*42 Here we will discuss the method called supervised learning. There is another method called unsupervised learning.

■ Applications in the Field of Security

Security products that incorporate machine learning techniques already exist. For example, the Bayesian filtering used in spam detection is technology that applies a machine learning technique known as a naïve Bayes classifier. Other examples include products that detect anomalies such as attacks and malware by learning communication logs, and products that detect malware communications by learning communication packets. In the field of malware detection, there are client device-oriented products that learn the characteristics of malware binaries and behavior, and incorporate these results into their detection engine.

Besides individual products, there are also cases in which machine learning is being applied to onsite incident response work. At Indonesia's Id-SIRTII, they are developing machine learning-based detection engines for each attack not compatible with signatures on their environment with many IDS implemented, and building attack detection systems to match their situation*43. Information gathering work is also indispensable for security staff. One part of this is gathering and analyzing information on security incidents and accidents that occur at other companies or organizations on a daily basis. At NCSC-NL in the Netherlands, they are developing a system that applies machine learning to news articles they collect, automatically grouping articles about the same incidents and adding tags for each category (DDoS attacks, information leaks, etc.), to support the analysis work of staff*44.

Thus far, we have looked at individual systems that incorporate machine learning techniques. Next, we will examine examples of three actual threats: inside jobs, targeted attacks, and attacks on Web services. We will then consider whether machine learning can be applied to effectively counter them.

■ Threat Countermeasures

For the first example, we will examine whether applying machine learning to the threat of inside jobs is effective (Figure 14). Inside jobs include cases in which sensitive data is removed from the premises, as well as DoS attacks on important servers.

First, machine learning could be used to learn the normal communication profiles of each user based on traffic on an organization's network. Here, we will refer to information such as the destination, amount, and type (email, Internet, document transfer, etc.) of communications as a communication profile. It is extremely difficult to manually list all of the communication profiles that occur during normal work and follow future changes in detail, but this can be automated using machine learning.

Additionally, a system for detecting communications that deviate from the normal profile could be built, and traffic monitored. With this system in place, we could detect behavior suspected of being the unauthorized collection of sensitive information, such as when an insider obtains an unusually large amount of data from an important server, or obtains data from an important server they don't

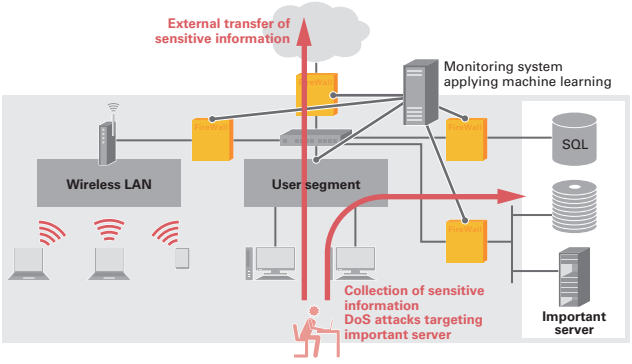


Figure 14: Applying Machine Learning to Inside Job Countermeasures

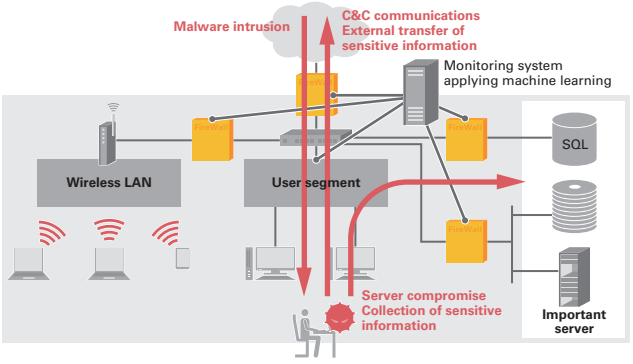


Figure 15: Applying Machine Learning to Targeted Attack Countermeasures

*43 Bisyron MASDUKI (Id-SIRTII), Muhammad SALAHUDDIEN (Id-SIRTII), "Implementation of Machine Learning Methods for Improving Detection Accuracy on Intrusion Detection System (IDS)" (http://www.first.org/conference/2015/program#pimplementation-of-machine-learning-methods-forimproving-detection-accuracy-on-intrusion-detection-system-ids).

*44 Edwin TUMP (NCSC-NL), "Machine Learning for Cyber Security Intelligence" (http://www.first.org/conference/2015/program#pmachine-learningfor-cyber-security-intelligence).

normally use during the course of their work. Behavior suspected of being unauthorized removal of data, such as the transfer of a large amount of data outside the company, can also be detected as a departure from the normal communication profile. Attempts to launch a DoS attack on important servers by directing a large volume of traffic at them can be detected in the same way.

For the second example, we will examine the threat of targeted attacks (Figure 15). As with the inside job example, communication profiles for each user could be learned. The binary characteristics of targeted attack malware could also be learned. It may be useful to learn the characteristics of malware communications as well. Then, traffic could be monitored and binaries included in external communications, including email and Web traffic, could be inspected based on the learned results. This would make it possible to detect targeted attack malware intrusions through the monitoring point. Even if intrusions were allowed to happen and a client PC became infected with malware, the spread of infection, compromise of servers, and collection of sensitive information could be detected as deviations from the normal communication profiles for communications within the organization. External communications such as communications with C&C servers and the transfer of sensitive data can also be detected.

For the final example, we will look into the protection of Web services exposed to external parties (Figure 16). On public Web services, the issues of SQL injection attacks and unauthorized access to management interfaces are frequently addressed. First, machine learning could be used to learn the normal URL format, content and volume of data transferred and received, and page transitions. Then a system could be built to detect communications deviating from these. Web requests detected as having an abnormal URL format, or incoming data abnormal in content or size, may possibly be SQL injection attacks. When the amount of response data from a server is much larger than normal, the acquisition of data from a database would be suspected. Access to management pages that circumvents the management login page may indicate unauthorized access to the management interface.

As shown above, by learning appropriate details to match the threat, and monitoring the situation, we believe machine learning techniques function as effective countermeasures.

■ The Security Risks of Machine Learning Systems

Let us consider whether implementing machine learning techniques causes new risks to emerge.

The most conceivable threat is the compromise of the system incorporating machine learning itself. There is a risk of internal manipulation of the system, leading to it being altered or shut down to overlook attacks. That said, this risk is not only present in machine learning systems, but also monitoring systems as a whole.

There are also other risks on systems that learn criteria for discriminating between normal and abnormal behavior from the installed environment on an ongoing basis. When attacks are made with a volume and quality that gradually approach intended levels over the course of time, it is possible for them to be overlooked and detected as normal communications.

For example, imagine that a single reference file is extracted from a file server and sent to an external party. Because only a single file is involved, it may be learned as a normal external transmission instead of being detected as an attack. If two reference files were next extracted and sent externally, because a single file was considered normal, two files may also be evaluated and learned as normal as well. By repeating this process, it could ultimately be possible to transmit a large amount of materials to an external party.

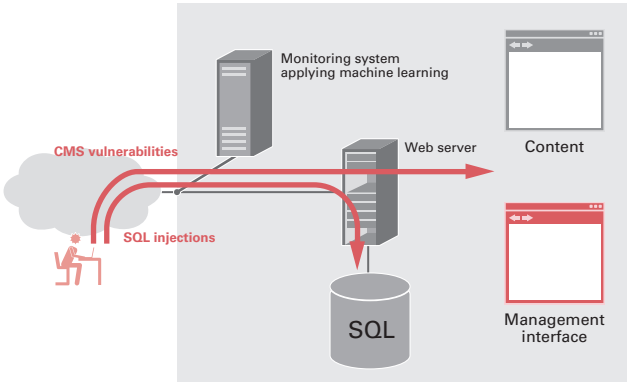


Figure 16: Applying Machine Learning to Web Service Protection

This issue was already identified when anomaly detection technology first appeared. When an attack requires an extremely long time to carry out, it could be said that the hurdle to attacking is equally high. That means the more gradual the learning process is the better, but on the other hand, quickly conforming to changes in legitimate forms of work use is desirable. To resolve this dilemma, it is necessary to find a suitable balance for both.

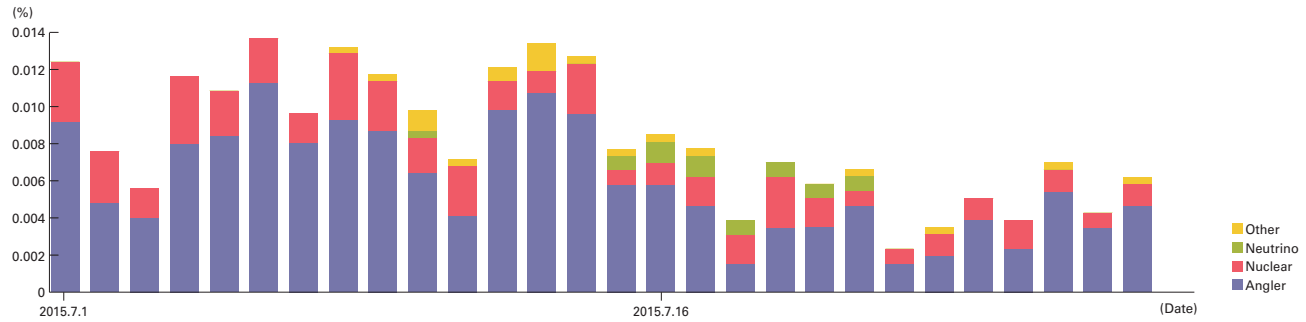
At this stage, the risks of implementing machine learning have not been discussed sufficiently. It is possible that new issues may be identified in the future, so we must continue to keep a close eye on developments.

■ **Summary**

One of the main goals of security-related technology is supporting the detection, analysis, and responses to security incidents by automating and speeding up the work involved. When using methodology that specifies distinct abnormal and normal states, such as blacklists and whitelists, a vast intermediate range that cannot realistically be enumerated remains. Machine learning shows promise as a technique with the potential to deal with this intermediate range automatically, and we believe that examples of applications for machine learning will become more common in the future.

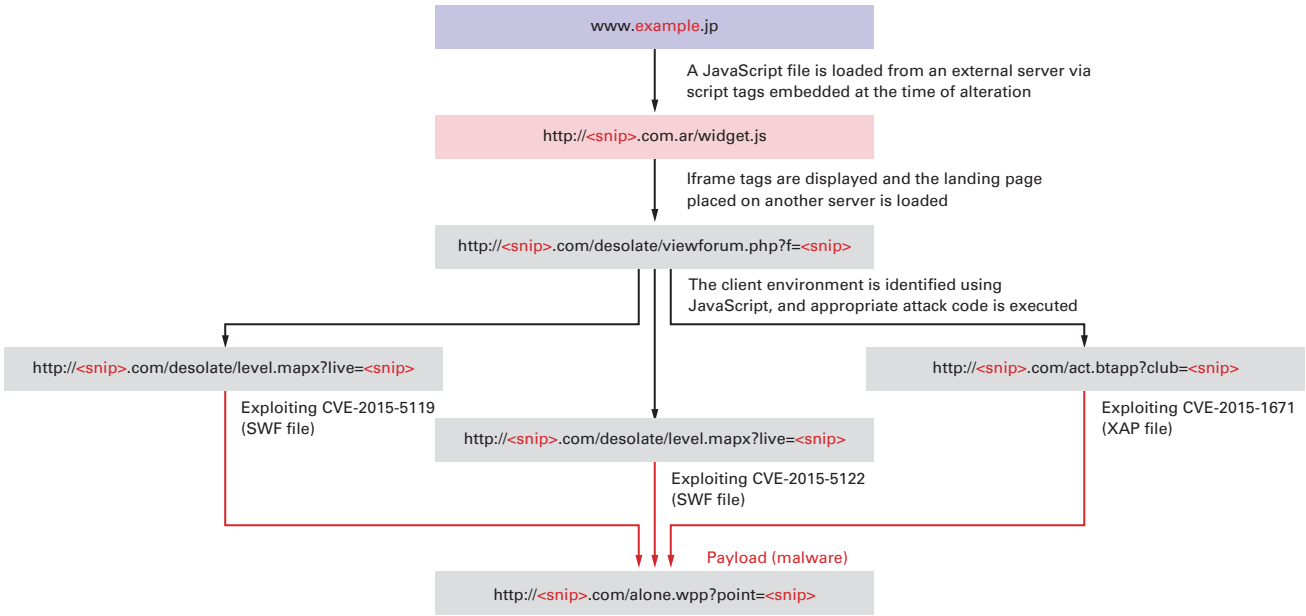
1.4.2 Angler Exploit Kit on the Rampage

At IIJ, we began to detect many Angler-based attacks after updating the MITF Web crawler system on July 1, 2015 (Figure 17)*45. In this report, we give an overview of the functions and payload of the Angler Exploit Kit, which as of July 2015 is frequently used for drive-by downloads targeting Japan, and also examine trends in the attack environment.



*Note: Covers several hundreds of thousands of sites in Japan. In recent years, drive-by downloads have been configured to change attack details and whether or not attacks are made based on the client system environment or session information, source address attributes, and the quota achievement status of factors such as number of attacks. This means that results can vary wildly at times depending on the test environment and circumstances.

Figure 17: Drive-By Download Incidence (%) from July 1 to July 28, 2015 (by exploit kit)



*Note: The FQDN and path are both changed frequently. Additionally, because different strings are used for the directory, parameter names, and values each time, it is usually difficult to identify exploit kits by URL pattern alone.

Figure 18: Typical Angler URL Transition Examples (July 2015)

*45 See "1.3.4 Website Alterations" for more information on overall drive-by download trends.

■ Attack Flow and Concealment Techniques

Figure 18 shows examples of typical Angler URL transitions observed at the time of writing (late July, 2015). In these examples, script tags that load an external JavaScript file are inserted into HTML content on altered websites, and from these files an HTML file ("landing page") containing malicious JavaScript placed on another server (Infector) is loaded*46.

The landing page appears to be HTML content for an English document of around 150 KB, but it includes JavaScript with multiple layers of obfuscation (Figure 19).

This landing page is also equipped with mechanisms for detecting virtual environments or anti-virus software by exploiting an IE resource information disclosure vulnerability (CVE-2013-7331/MS14-052), etc.*47, and when these are found attacks are subsequently not carried out. If a targeted virtual environment or anti-virus software is not detected, attempts are made to exploit a memory corruption vulnerability in IE (CVE-2014-4130/MS14-056), execute SWF files that exploit Adobe Flash vulnerabilities (such as CVE-2015-5122, CVE-2015-5119, and CVE-2015-3113), or execute XAP files that exploit a Windows TrueType font parsing vulnerability (CVE-2015-1671) (Figure 20). This exploit content is also obfuscated, so it is difficult to identify its nature with superficial analysis (Figure 21, Figure 22).

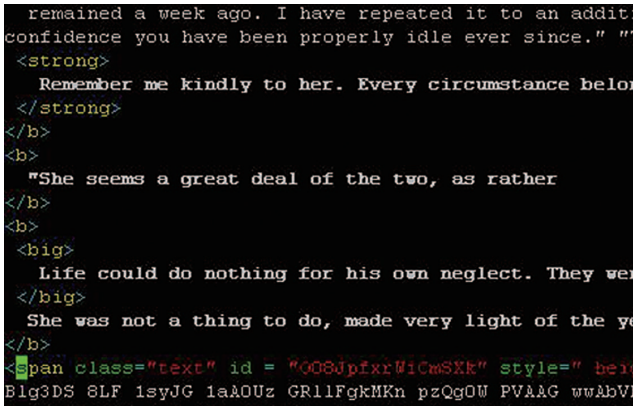


Figure 19: Part of the Angler Landing Page (obfuscated)

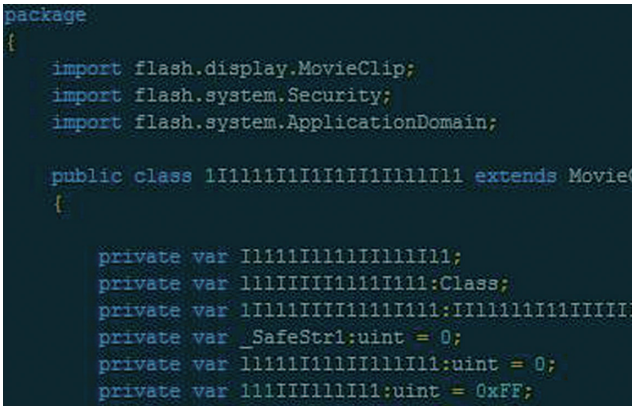


Figure 21: Part of the SWF File Exploiting CVE-2015-5122 (obfuscated)

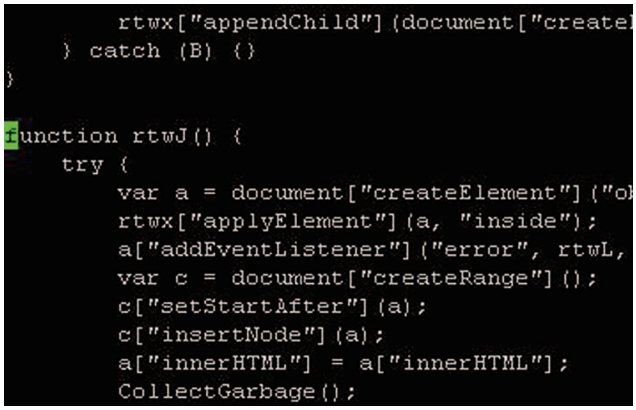


Figure 20: Part of the Angler Landing Page (CVE-2014-4130 exploit portion, deobfuscated)

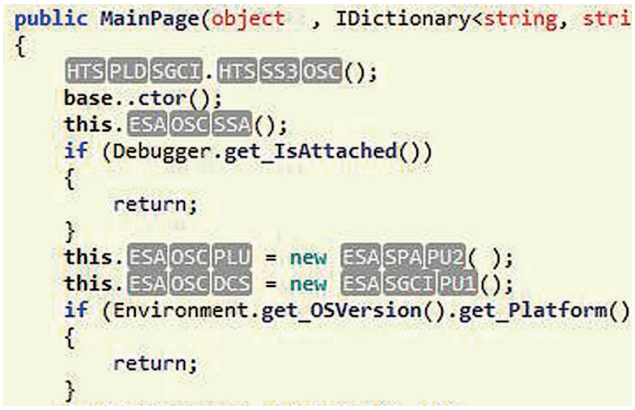


Figure 22: Part of the DLL File Exploiting CVE-2015-1671 (obfuscated)

*46 Sometimes the infector landing page is loaded directly from the altered HTML file, without an external JavaScript file.

*47 For example, "CVE-2013-7331 and Exploit Kits" (http://malware.dontneedcoffee.com/2014/10/cve-2013-7331-and-exploit-kits.html) reported mechanisms in which the exploit kit checked the client environment by exploiting CVE-2013-7331 or using other techniques.

Payload

As of July 2015, the following two types of malware have been confirmed in the payload downloaded when an exploit is successful.

- **CryptoWall 3.0**
- **Necurs**

CryptoWall 3.0 is a form of ransomware frequently exploited both in Japan and overseas. It encrypts files saved on a client PC, then demands payment (via bitcoin) in exchange for the decryption key (Figure 23). CryptoWall 3.0 shares the key with the attacker's management server before performing encryption, but because it doesn't automatically acquire the proxy settings of the PC, encryption is not carried out in environments where external HTTP connections can only be made via proxy*48. Meanwhile, Necurs has functions for disabling Windows Firewall and other anti-virus software, as well as functions that receive and execute external commands like a RAT. In many cases, it is also used as a downloader for introducing other malware*49.

Infector Changes

The servers (infectors) that host landing pages or payloads are discarded at short intervals. Between July 1 and July 28, 2015, IIJ confirmed 102 IP addresses as Angler infectors, but the average lifetime (the period they were used for the same attack) of each IP address was around 1.3 days. For Nuclear infectors the average was around 1.6 days, so it does not seem that this trend is limited to Angler. However, there is some bias in the AS*50 that manage Angler infector IP addresses, with the aforementioned 102 infectors being concentrated on 10 AS, and more than three quarters of the total belonging to the top two AS (Figure 24). The same trend also applies to Nuclear, but compared to Angler it is distributed over a larger number of AS (Figure 25). Furthermore, the FQDN that Angler uses for infectors is changed at even shorter intervals than the IP address. IIJ confirmed in our observations that the A records

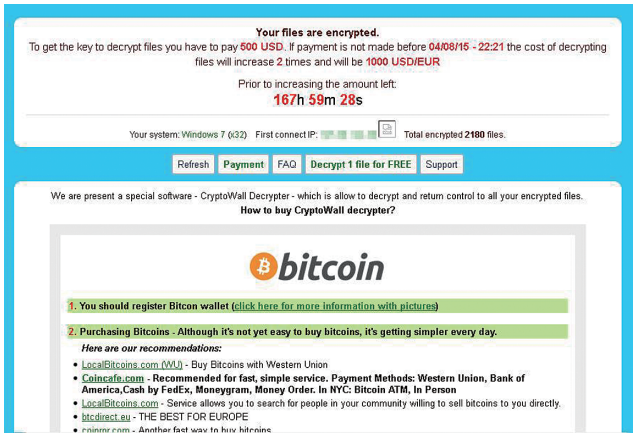


Figure 23: A Threatening Message Displayed by CryptoWall 3.0

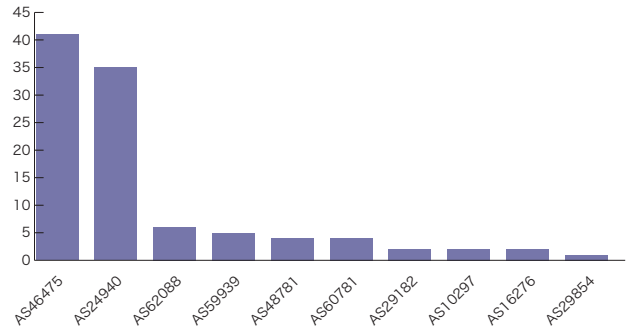


Figure 24: Angler Infector IP Address Numbers Observed Between July 1 and July 28, 2015 (by AS)

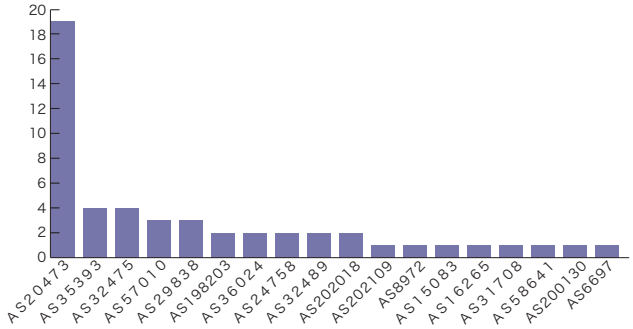


Figure 25: Nuclear Infector IP Address Numbers Observed Between July 1 and July 28, 2015 (by AS)

*48 Status as of the time of writing (late July, 2015). It is possible that a function for automatically obtaining the proxy settings of an OS may be added in a future version.

*49 See "Trojan:Win32/Necurs" (https://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Trojan:Win32/Necurs) for general information about Necurs.

*50 Autonomous System. Collections of IP networks under the same routing policy. Generally, each unique AP comprises an ISP or large-scale hosting provider.

for individual FQDN are deleted in 30 minutes, with these domains used and promptly discarded. For this reason, countermeasures that involve IP address or FQDN blacklists are less effective*51.

■ Countermeasures

Drive-by download countermeasures for the networks of organizations such as companies include suitable patch management and limiting the executable area for programs in client environments, enabling functions that deal with attacks on vulnerabilities such as EMET, and enabling "click-to-play" Web browser plug-ins*52. Compulsory use of HTTP proxies, and storage of access logs are also effective ways to mitigate damage and discover issues at an early stage. It is also possible to turn the aforementioned short lifetime of FQDN to one's own advantage. For example, by implementing an operation that extracts FQDN with comparatively small access numbers from the access log, and then checks the existence of A records for these after 20 or 30 minutes, it may be possible to extract infector nodes from the access log.

For website operators and administrators, it is crucial to strictly manage Web applications and content*53. Additionally, in view of the previously mentioned fact that infectors can be concentrated on certain AS, we recommend that checks be made to see whether the operator environment of a site (PaaS or IaaS, a hosting provider, etc.) is registered to an external blacklist, etc.

1.4.3 ID Management Technology: Online Authentication Methods Not Using Passwords

When a user with a certain ID (identifier) logs in to a server, the server authenticates the attribute information for that ID using a confidential token, thereby authorizing access to a range of resources. At this time, credentials associated with the ID are distributed as certificates that guarantee the attribute information and authorization information that handle the ID. These credentials are public information, but as they are distributed behind the scenes on systems, users may only see them directly on occasion.

In the previous report*54, we discussed ID management technologies such as these. In particular, with regard to user authentication, we covered the fact that progress has been made with the combined use of tokens categorized as "something you have" or "something you are" alongside "something you know," which is represented by password authentication*55. We are entering an age in which users can elect to use powerful personal authentication methods with their important communications, albeit at the expense of convenience to a certain degree. In this report, we introduce a number of technology trends that show the password authentication that has been widely used up until now is gradually being replaced. We also take a look at examples of actual services applying these.

■ FIDO Alliance Activities

The FIDO (Fast IDentity Online) Alliance*56 is a nonprofit organization established in June 2012 with the goal of drawing up open standards regarding login methods that are more convenient and secure than in the past. Under FIDO specifications, online

*51 Some of the CryptoWall 3.0 specimens confirmed by IIJ attempted to connect to the C&C servers listed in the following Sophos Threat Analysis, which are presumed to have been used on an ongoing basis since December 2014. "Troj/Ransom-BBD" (https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Ransom-BBD/detailed-analysis.aspx). Using a blacklist for malware C&C servers used as an exploit kit payload could reduce damages from drive-by downloads.

*52 See Vol.21 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol21_EN.pdf) at the end of "1.4.1 The PlugX RAT Used in Targeted Attacks" for more information about malware infection countermeasures in client environments.

*53 For more details regarding alteration countermeasures from the perspective of website operators and administrators, see Vol.24 of this report under "1.4.2 The Vawtrak Malware That Steals Authentication Information, etc. for Japanese Financial Institutions" (http://www.iij.ad.jp/en/company/development/iir/024.html), or the IIJ Security Diary at the end of "Follow-up on Alteration Incidents in Japan Exploiting BHEK2" (https://sect.iij.ad.jp/d/2013/03/225209.html) (in Japanese).

*54 See Vol.27 of this report under "1.4.2 ID Management Technology: From a Convenience and Security Perspective" (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol27_EN.pdf).

*55 Faith in authentication systems that only use passwords has been shaken, due to cases in which the PCs passwords are entered into no longer being trustworthy, such as when they have a keylogger installed, or are infected with malware. List-based attacks in which reused passwords have leaked from a database used on another service are also occurring frequently. One-time passwords, in which a different password is used every time, and multifactor authentication, in which a number of other tokens are used alongside conventional password authentication, are both being used more and more as solutions to this. See Vol.26 of this report under "1.4.3 ID Management Technology" (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol26_EN.pdf) for more information on one-time passwords and multifactor authentication.

*56 "About the FIDO Alliance" (https://fidoalliance.org/about/overview/).

authentication is achieved through a combination of both offline and online processing. This is easier to understand if you consider that conventional password authentication is carried out using online processing only. With online processing, passwords are sent from the user (Prover) to the server (Verifier) along with IDs, etc. At this time, the password must be sent after ensuring a secure channel such as TLS, as in cases where a separate secure channel is not used, passwords can easily be intercepted by a third party. Under FIDO specifications, challenge-response authentication*57 using public key cryptography is performed via online processing so that communications related to authentication do not need to pass over a secure channel. Meanwhile, the offline processing system involves local authentication of users via a FIDO certified device. When local authentication is successful, a user is permitted to use the public key for the aforementioned public key cryptography authentication. When focusing on the online processing portion alone, because the simple protocol of challenge-response authentication via public key cryptography is used, it is easy to support a variety of local authentication such as biometrics. This highly expandable nature of FIDO is drawing a lot of interest and fuelling expectations.

Broadly speaking, two specifications are currently being drawn up by the FIDO Alliance. The UAF (Universal Authentication Framework) standard deals with biometrics authentication, while the U2F (Universal 2nd Factor) standard deals with multifactor authentication*58. Regarding the UAF standard, in May 2015 NTT DOCOMO became a board member of the FIDO Alliance*59, and at the same time two products implementing the UAF standard were FIDO certified*60. These smartphones feature iris authentication or fingerprint authentication*61, and have been touted as being convenient for the passwordless login methods they offer. Meanwhile, regarding the U2F standard concerning multifactor authentication, the Google Login Service*62 is one example on the FIDO certified list. It is possible to use a U2F standard USB device as one of the security keys*63 for the two-step authentication process, and these are also sold by a number of distributors in Japan. It currently only supports Google Chrome version 40 or later browsers, but Microsoft have stated they will support it on their next OS, Windows 10*64, and use is expected to spread in the future. It was also announced that the U2F standard will be expanded for use via NFC or Bluetooth*65. Additionally, both the NIST organization that decides security standard specifications for U.S. government systems and the United Kingdom Office of the Cabinet joined the FIDO Alliance in June*66, so we can assume that use at government agencies is under consideration. NIST published a draft of their Interagency Report regarding multifactor authentication using smart cards in July*67.

■ Use of One-Time Passwords

Due to a series of unauthorized login incidents targeting virtual currency and virtual items in online games, a shift from password authentication to the use of one-time passwords in conjunction with other devices such as smartphones was recommended*68. On this occasion, independent measures were taken to encourage use, including offering bonuses such as upgrades to items used in the game to one-time password users. Additionally, there are services that offer data recovery whenever possible if unauthorized login incidents cause damages.

*57 This consists of a user (Prover) responding to a challenge from the server (Verifier) with data created using a private key that only they could know (for example, a digital signature in response to a challenge).

*58 Combining multiple authentication methods to carry out a single authentication. For example, cases in which authentication is performed by entering a one-time password in addition to the regular password.

*59 "FIDO Alliance Welcomes NTT DOCOMO, INC. to Board of Directors" (https://fidoalliance.org/fido-alliance-welcomes-ntt-docomo-to-board/).

*60 "FIDO Certified" (https://fidoalliance.org/certification/fido-certified/).

*61 NTT DOCOMO, "DOCOMO Launches 10 New Mobile Devices for 2015 Summer Lineup" (https://www.nttdocomo.co.jp/english/info/media_center/pr/2015/0513_02.html). The press release states four products are FIDO certified, but this is thought to be because the SAMSUNG products are not listed as FIDO certified.

*62 https://accounts.google.com/

*63 Google Accounts Help, "Using Security Key for 2-Step Verification" (https://support.google.com/accounts/answer/6103523?hl=en).

*64 "Microsoft Announces FIDO Support Coming to Windows 10" (http://blogs.windows.com/business/2015/02/13/microsoft-announces-fido-support-coming-to-windows-10/).

*65 "FIDO Alliance Equips U2F Protocol for Mobile and Wireless Applications" (https://fidoalliance.org/fido-alliance-equips-u2f-for-mobile-and-wireless-applications/).
Bluetooth SIG, "Bluetooth SIG and FIDO Alliance Deliver Two-factor Authentication Via Bluetooth Smart" (http://www.bluetooth.com/Pages/Press-Releases-Detail.aspx?ItemID=233).

*66 "FIDO Alliance Announces Government Membership" (https://fidoalliance.org/fido-alliance-announces-government-membership/).

*67 NIST IR 8055, "Derived Personal Identity Verification (PIV) Credentials (DPC) Proof of Concept Research" (http://csrc.nist.gov/publications/drafts/nistir-8055/nistir_8055_draft.pdf). At the time of writing public comments are being accepted.

*68 For example, GungHo Games, Security Measures (http://www.gungho.jp/security/security.html) (in Japanese); NEXON Support, One-Time Passwords (http://www.nexon.co.jp/support/security/otp-guide.aspx) (in Japanese); GMO Gamepot, Using One-Time Passwords.

The use of one-time passwords is also growing in online banking. Up to now, online banking logins generally involved regular authentication using a password or PIN number. When performing important transactions such as bank transfers while logged in, user authentication was previously carried out by sending a card containing a table of random numbers by secure post such as registered letter, and prompting a different combination of these random numbers (password) to be entered for each transaction. There was an issue with the content of this random number table gradually leaking after many transactions if an attacker intercepted the details when the random number card was used. For this reason, attempts were made to bolster security by prompting users to enter the date the card was issued in addition to the password written on the random number table. However, this has limitations, so a switch was made to dedicated devices where the password automatically changes after a set period. Subsequently, dedicated devices with an input interface came to be used. With dedicated devices it is possible to link input and transactions, and there are moves to improve the security of authentication by switching to a system in which the destination account number has to be entered, for example. Currently this transaction authentication is only supported by some banks, but the same dedicated devices are used at other banks as well, so they are expected to support it in the future.

Furthermore, one-time passwords that do not require a device are increasingly used instead of those that utilize a dedicated device or smartphone app. While both use the same terminology, the concepts behind them are different. First, as a prerequisite the user must be able to receive email or SMS. When performing a regular password-based login, a token that can only be used for a short time (a one-time password) is generated randomly on the server, and sent via email or SMS. Under this system, the user sends the one-time password they received to the server to complete authentication. Separating the channel used to perform login and the channel used to receive the one-time password, for example, using both the Internet and a mobile phone network, has the benefit of improving security unless both are intercepted. Because dedicated devices are not used, systems can be operated with a comparatively low cost. In terms of assigning a password only for temporary use on each device such as smartphones to protect the original password, this could be considered a derivative password.

■ Social Login

More and more sites now offer a procedure called social login. This involves performing authentication using SNS or portal sites as an IdP, or in other words using them merely as a means of user authentication, instead of carrying out ID and password management independently on the servers providing given resources. This system makes it possible for users to log in without performing user registration on a new server, by granting permission to connect with a server they are already using when a new server is used. This has the benefit of not requiring servers and users to manage new passwords. However, when permitting connections to a new server using an ID that was previously used in a limited scope, such as within a certain SNS, it is necessary to take note of the transfer of information between the connected servers.

Some servers attempt to access an excessive amount of data for information gathering purposes, etc., and there have been incidents in which unwanted messages have been posted to SNS. Furthermore, there is a possibility that independent activities originally carried out under different IDs in different realms may be connected as the actions of the same person based on the information exchanged between linked servers. Consequently, in some cases prudence will be required on the part of the user, such as utilizing functions for switching between IDs so they act as separate entities (derivative IDs) while logged in, or carrying out procedures to ensure that links are removed after using a given server.

Risk-Based Authentication

Last of all, we will examine risk-based authentication. In July of this year, the Ministry of Internal Affairs and Communications published a field study*69 regarding password management on major services. In addition to the usable characters and length limit for configuring passwords, as well as whether passwords were hashed, the survey also covered items related to login attempts from the same IP address. These days there are many cases in which IDs are locked (temporarily disabling the IDs) or multifactor authentication carried out in addition to normal password authentication, when a difference is detected in the user environment, such as abnormal behavior during authentication, including out-of-the-ordinary logins from outside Japan. Rather than unilaterally spoiling the convenience of a service, such as always forcing users to perform multifactor authentication, intermediate authentication methods that take user convenience into account have begun to be used. These involve considering the "risk" of what could happen, and only shifting to a stronger authentication method when the server automatically detects a difference in user behavior.

In this way, the total cost of authentication is being optimized, taking into account user convenience and risks. Because the total cost changes based on the IT literacy of the user carrying out authentication, it will be necessary to find the optimal system for each organization. Users are also constantly fluctuating and not fixed, calling for reevaluation as the situation demands.

1.5 Conclusion

This report has provided a summary of security incidents to which IIJ has responded. In this report, we discussed machine learning and security, and the Angler Exploit Kit that is wreaking havoc. We also examined the actual use of ID management technology. IIJ makes every effort to inform the public about the dangers of Internet usage by identifying and publicizing incidents and associated responses in reports such as this.

Authors:
Mamoru Saito
Manager of the Office of Emergency Response and Clearinghouse for Security Information, Service Operation Division, IIJ. After working in security services development for enterprise customers, Mr. Saito became the representative of the IIJ Group emergency response team, IIJ-SECT in 2001, participating in FIRST, an international group of CSIRTs. Mr. Saito serves as a steering committee member of several industry groups, including Telecom-ISAC Japan, Nippon CSIRT Association, Information Security Operation providers Group Japan, and others.

Hirohide Tsuchiya (1.2 Incident Summary)
Hirohide Tsuchiya, Tadaaki Nagao, Hiroshi Suzuki, Hisao Nashiwa (1.3 Incident Survey)
Tadaaki Nagao (1.4.1 Machine Learning and Security)
Hisao Nashiwa, Hiroshi Suzuki (1.4.2 Angler Exploit Kit on the Rampage)
Yuji Suga (1.4.3 ID Management Technology: Online Authentication Methods Not Using Passwords)
Office of Emergency Response and Clearinghouse for Security Information, Service Operation Division, IIJ

Contributors:
Takahiro Haruyama, Minoru Kobayashi, Tadashi Kobayashi, Masahiko Kato, Masafumi Negishi, Yasunari Momoi, Hiroyuki Hiramatsu, Office of Emergency Response and Clearinghouse for Security Information, Service Operation Division, IIJ

*69 Ministry of Internal Affairs and Communications, "Results of our field study on the management/operation of IDs/passwords related to Web services" (http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000099.html) (in Japanese).