1. Infrastructure Security

Route Hijacking

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 July 1 through September 30, 2015. In this period a number of hacktivism-based attacks were once again carried out by Anonymous and other groups, and there were frequent incidents that included many DDoS attacks, information leaks caused by unauthorized access, and website defacements. In an incident in which an Italian security firm was attacked, 400 GB of internal information was leaked, including the details of vulnerabilities in a number of other companies' software products for which no fixes were available until the vendors fixed them later. There was also a rash of incidents of unauthorized access and resulting information leaks and website alterations. In several incidents in Japan, websites were exploited as stepping stones in targeted attacks. 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 July 1 and September 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.

During this survey period, individuals and organizations thought to be associated with ISIL or sympathetic to its principles continued to carry out website defacements and SNS account hijackings around the world. In July, the website of a human rights watchdog in Syria was defaced. Defacements were also made to a NATO-related site in Georgia for supporting Jordan, and Malaysian police accounts on SNS sites such as Facebook and Twitter were hijacked. A number of other attacks were made on the Internet in response to circumstances and unrest caused by conflicts or diplomatic issues.

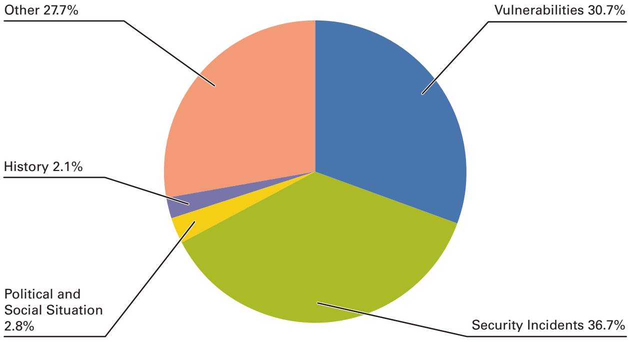


Figure 1: Incident Ratio by Category
(July 1 to September 30, 2015)

Multiple attacks were also made in protest against the government-led regulation of the Internet and communications. In Canada, there were incidents such as DDoS attacks and leaks of internal information due to the compromise of servers at a number of government agencies, including local administrative bodies, stemming from outcry against an anti-terror bill passed into law in June (OpC51). In India, a telecommunications carrier funded by the Indian government was accessed without authorization, leading to damages including the leak of account information for over 30 million users, in protest against government moves to strengthen Internet regulations in India (OpIndia). In Vietnam, Government-related websites were defaced in protest against online censorship carried out by the government. Similarly, the

[*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.

website of the National Telecommunications Commission in the Philippines was also defaced. In Thailand, DDoS attacks were made on a number of government-related websites in protest against stricter national censorship of communications.

In Japan, DDoS attacks thought to have been perpetrated by Anonymous as part of protests against the drive hunting of dolphins and small whales temporarily rendered the website of Taiji-cho in Wakayama Prefecture inaccessible (OpKillingBay). Attacks associated with this operation continued into October, targeting the websites of related organizations, government agencies, airports, and news outlets. Because attacks have also spread to organizations without a clear connection to the protests at the time of writing, caution must be exercised.

In Canada, there were DDoS attacks targeting the Royal Canadian Mounted Police (RCMP) after they shot to death a member of Anonymous who was protesting the construction of a dam for hydroelectric power generation. The Canadian Security Intelligence Service (CSIS) was also compromised, leading to the leak of classified internal documents to the press. In the United States, the United States Census Bureau was accessed without authorization and personal information for around 4,200 employees leaked in protest against negotiations for the Trans-Pacific Partnership (TPP).

Other attacks by hacktivists such as Anonymous continued on government and government-related websites around the world.

■ Vulnerabilities and their Handling

During this period, fixes were released for the Edge[*2][*3] browser new to Microsoft's Windows 10, which was released in July. There were also fixes for Windows[*4][*5][*6][*7][*8][*9][*10], Internet Explorer[*11][*12][*13], and Office[*14][*15][*16]. Updates were also made to Adobe Systems' Flash Player, Shockwave Player, Acrobat, and Reader. A quarterly update was released for Oracle's Java SE, fixing many vulnerabilities. A large number of vulnerabilities were also fixed in Apple's OS X. 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. Vulnerabilities in BIND DNS servers that could allow DoS attacks by external parties via the receipt of specially-crafted queries were also discovered and fixed. A number of vulnerabilities in the Apache Struts 2 Web

[*2] "Microsoft Security Bulletin MS15-091 - Critical: Cumulative Security Update for Internet Explorer (3084525)" (https://technet.microsoft.com/library/security/ms15-091).

[*3] "Microsoft Security Bulletin MS15-095 - Critical: Cumulative Security Update for Microsoft Edge (3089665)" (https://technet.microsoft.com/library/security/ms15-095).

[*4] "Microsoft Security Bulletin MS15-066 - Critical: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (3072604)" (https://technet.microsoft.com/library/security/ms15-066).

[*5] "Microsoft Security Bulletin MS15-067 - Critical: Vulnerability in RDP Could Allow Remote Code Execution (3073094)" (https://technet.microsoft.com/library/security/ms15-067).

[*6] "Microsoft Security Bulletin MS15-068 - Critical: Vulnerabilities in Windows Hyper-V Could Allow Remote Code Execution (3072000)" (https://technet.microsoft.com/library/security/ms15-068).

[*7] "Microsoft Security Bulletin MS15-077 - Important: Vulnerability in ATM Font Driver Could Allow Elevation of Privilege (3077657)" (https://technet.microsoft.com/library/security/ms15-077).

[*8] "Microsoft Security Bulletin MS15-080 - Critical: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3078662)" (https://technet.microsoft.com/library/security/ms15-080).

[*9] "Microsoft Security Bulletin MS15-097 - Critical: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3089656)" (https://technet.microsoft.com/library/security/ms15-097).

[*10] "Microsoft Security Bulletin MS15-098 - Critical: Vulnerabilities in Windows Journal Could Allow Remote Code Execution (3089669)" (https://technet.microsoft.com/library/security/ms15-098).

[*11] "Microsoft Security Bulletin MS15-065 - Critical: Security Update for Internet Explorer (3076321)" (https://technet.microsoft.com/library/security/ms15-065).

[*12] "Microsoft Security Bulletin MS15-079 - Critical: Cumulative Security Update for Internet Explorer (3082442)" (https://technet.microsoft.com/library/security/ms15-079).

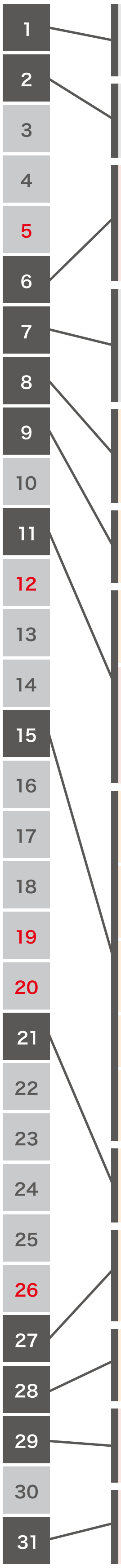
[*13] "Microsoft Security Bulletin MS15-094 - Critical: Cumulative Security Update for Internet Explorer (3089548)" (https://technet.microsoft.com/library/security/ms15-094).

[*14] "Microsoft Security Bulletin MS15-070 - Important: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3072620)" (https://technet.microsoft.com/library/security/ms15-070).

[*15] "Microsoft Security Bulletin MS15-081 - Critical: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3048019)" (https://technet.microsoft.com/library/security/ms15-081).

[*16] "Microsoft Security Bulletin MS15-099 - Critical: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3089664)" (https://technet.microsoft.com/library/security/ms15-099).

July Incidents



O **1st: A leap second was inserted to adjust Coordinated Universal Time at 8:59:60 AM Japan time.**
National Institute of Information Communications Technology (NICT), "July 1, 2015, is one second longer" (http://jjy.nict.go.jp/news/leap-info2015.html) (in Japanese).

O **2nd: The Financial Services Agency published its "Policy Approaches to Strengthen Cyber Security in the Financial Sector," which outlined five policies aimed at bolstering cyber security in the field of finance.**
"Publication of the Policy Approaches to Strengthen Cyber Security in the Financial Sector" (http://www.fsa.go.jp/en/news/2015/20151105-1.html).

S **6th: An incident occurred in which Italian security firm Hacking Team was compromised by an unknown party, and 400 GB of internal data leaked to P2P networks. Because the internal information leaked included details of vulnerabilities in software such as Flash Player for which no fix was available that Hacking Team had in its possession, there have been a number of attacks exploiting these vulnerabilities.**
See the following Hacking Team announcement for more information about this incident. "Information related to the attacks on Hacking Team on July 6, 2015" (http://www.hackingteam.com/index.php/about-us).

O **7th: Due to issues with the unauthorized use of phone services such as IP phones that caused users to be billed for expensive international telephone charges, the Ministry of Internal Affairs and Communications asked for the cooperation of telecommunications carrier organizations in advising users to take measures to prevent such damages caused by unauthorized use and stop their spread.**
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).

V **8th: A vulnerability in BIND9 that could allow DoS attacks from outside under certain conditions, such as when DNSSEC verification is enabled, was discovered and fixed.**
Internet Systems Consortium, "CVE-2015-4620: Specially Constructed Zone Data Can Cause a Resolver to Crash when Validating" (https://kb.isc.org/article/AA-01267).

V **9th: A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination or arbitrary code execution when a specially-crafted website is viewed were discovered and fixed.**
"APSB15-16: Security updates available for Adobe Flash Player" (https://helpx.adobe.com/security/products/flash-player/apsb15-16.html).

V **11th: A vulnerability (CVE-2015-5122) in Adobe Flash Player that could allow unauthorized termination or arbitrary code execution when a specially-crafted website is viewed was disclosed. A fix for this vulnerability (APSB15-18) was released on July 15.**
"APSA15-04 Security Advisory for Adobe Flash Player" (https://helpx.adobe.com/security/products/flash-player/apsa15-04.html).

S **11th: The U.S. Office of Personnel Management (OPM) published details on the current status of its investigation into an incident of unauthorized access that occurred in June, revealing that information on 21.5 million current, former, and future federal employees and independent contractors had leaked. They also announced they would establish a dedicated suite of services and a call center to deal with this issue.**
"OPM Announces Steps to Protect Federal Workers and Others From Cyber Threats" (https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/).

V **15th: Microsoft published their Security Bulletin Summary for July 2015, and released a total of 14 updates, including four critical updates such as MS15-065, MS15-066, and MS15-067, as well as 10 important updates.**
"Microsoft Security Bulletin Summary for July 2015" (https://technet.microsoft.com/library/security/ms15-jul).

V **15th: A number of vulnerabilities in Adobe Reader and Acrobat that could allow unauthorized termination and arbitrary code execution were discovered and fixed.**
"APSB15-15: Security Updates Available for Adobe Acrobat and Reader" (https://helpx.adobe.com/security/products/reader/apsb15-15.html).

V **15th: A number of vulnerabilities in Adobe Shockwave Player that could allow an attacker to take over control or execute arbitrary code were discovered and fixed.**
"Security update available for Adobe Shockwave Player" (https://helpx.adobe.com/security/products/shockwave/apsb15-17.html).

V **15th: A number of vulnerabilities in Adobe Flash Player that could allow arbitrary code execution were discovered and fixed.**
"APSB15-18: Security updates available for Adobe Flash Player" (https://helpx.adobe.com/security/products/flash-player/apsb15-18.html).

V **15th: Oracle released their quarterly scheduled update for a number of products including Oracle, fixing a total of 193 vulnerabilities, including 25 in Java SE.**
"Oracle Critical Patch Update Advisory - July 2015" (http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html).

V **21st: Microsoft released an unscheduled fix for a vulnerability (CVE-2014-2426) that could allow arbitrary code execution.**
"Microsoft Security Bulletin MS15-078 - Critical: Vulnerability in Microsoft Font Driver Could Allow Remote Code Execution (3079904)" (https://technet.microsoft.com/en-us/library/security/ms15-078.aspx).

V **27th: A vulnerability in Fiat Chrysler Automobiles (FCA) Uconnect that could allow a vehicle to be controlled remotely was discovered and fixed. This vulnerability only applied to products sold in the U.S., and the manufacturer issued a recall for that region.**
US-CERT, "Vulnerability Note VU#819439 Fiat Chrysler Automobiles Uconnect allows a vehicle to be remotely controlled" (https://www.kb.cert.org/vuls/id/819439).

V **28th: It was disclosed that Android Stagefright contained a number of vulnerabilities that could allow attackers to access files on a device or execute code.**
US-CERT, "Vulnerability Note VU#924951 Android Stagefright contains multiple vulnerabilities" (https://www.kb.cert.org/vuls/id/924951).

S **29th: There was a large-scale incident of malvertising that used the advertising network of U.S. Yahoo! to redirect users to the Angler Exploit Kit.**
See the following Malwarebytes Corporation blog post for more details. "Large Malvertising Campaign Takes on Yahoo!" (https://blog.malwarebytes.org/malvertising-2/2015/08/large-malvertising-campaign-takes-on-yahoo/).

S **31st: It was disclosed that someone had hijacked the email address for inquiries to the NPO support desk on the Cabinet Office NPO site, leading to emails being sent out without authorization.**
"[Important Notice] Regarding unauthorized use of the NPO support desk account" (https://www.npo-homepage.go.jp/uploads/20150731.pdf) (in Japanese).

*Dates are in Japan Standard Time

Legend V Vulnerabilities S Security Incidents P Political and Social Situation H History O Other application framework that could allow arbitrary code execution or XSS when certain conditions were fulfilled were discovered and fixed*[17]. A number of vulnerabilities that could allow sites to be compromised, including XSS vulnerabilities, were discovered and fixed in multiple versions of the WordPress CMS.

In July, a vulnerability*[18] was disclosed in the Uconnect in-car system for Fiat Chrysler Automobiles (FCA) vehicles that could allow remote control takeover of a vehicle, enabling third parties to perform actions such as braking and steering. Several Android device vulnerabilities that could allow arbitrary file access or code execution on devices by a remote attacker were discovered and fixed. Only an outline was published for these vulnerabilities at first, but the discoverers presented more details of each at Black Hat USA 2015, the world's largest security conference held in Las Vegas in August.

■ Information Leaks Due to Unauthorized Access

Incidents of unauthorized access and resulting information leaks continue to occur. In July, the U.S. medical institution UCLA Health announced that a computer network containing personal details such as names and medical histories had been compromised, and the personal information of around 4.5 million people may have leaked*[19]. In September, a U.S. medical insurance company was accessed without authorization, leading to the potential leak of 10.5 million pieces of personal data, including names and social security numbers. In an incident of unauthorized access that occurred at the U.S. Office of Personnel Management (OPM) in June, causing the leak of data on about 4 million federal employees, a subsequent investigation revealed that details of 21.5 million federal employees and independent contractors had actually leaked, and it is possible that fingerprint data of up to 5.6 million individuals had leaked as well*[20].

In Japan, the website of an education-related company was compromised in July, leading to the potential leak of personal information for up to 22,108 people. Also in July, the website of a travel-related company was accessed without authorization, and approximately 8,400 sets of email addresses and passwords for registered members may have leaked. Other incidents included a leak from the website of a toy company involving about 100,000 pieces of personal information registered to their online store. There were also many incidents of website compromise and resulting leaks of personal information due to the exploitation of application vulnerabilities, including SQL injections, affecting companies of all sizes in a range of fields, such as food and gift companies.

In addition to information leaks such as these caused by unauthorized access, since June websites for companies and organizations in Japan have also been compromised and altered to redirect users to malware, or exploited as C&C servers in targeted attacks. Due to this, IPA and JPCERT/CC have issued alerts with specific instructions regarding precautions to be observed for site operation, such as points that website administrators should check, and the frequency of inspection*[21].

■ 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 July, it was revealed that 36,300 pieces of data, including the personal information of students, may have leaked due to a PC used for work at a university being infected by malware attached to an email. In August, a malware infection caused by targeted emails from attackers posing as customers occurred at a railroad company, and it was disclosed that a number of business use PCs at the company had been infected with malware. Also in August, verification reports from a number of organizations were published regarding the leak of personal information from the Japan Pension Service in June. These summarized each of their perspectives on verification of the incident response as well as information security measures that should be bolstered to prevent future reoccurrence.

*17 The Apache Software Foundation, "Apache Struts 2 Documentation S2-025 Cross-Site Scripting Vulnerability in Debug Mode and in exposed JSP files" (https://struts.apache.org/docs/s2-025.html).

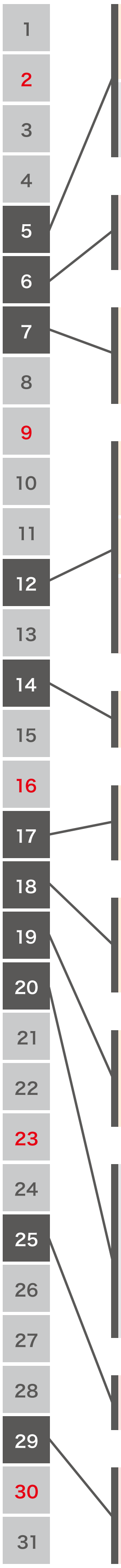
*18 See the following white paper from the person who disclosed the vulnerability for more information. "Remote Exploitation of an Unaltered Passenger Vehicle" (http://illmatics.com/Remote%20Car%20Hacking.pdf).

*19 UCLA Health, "UCLA Health Victim of a Criminal Cyber Attack" (https://www.uclahealth.org/news/ucla-health-victim-of-a-criminal-cyber-attack).

*20 "Statement by OPM Press Secretary Sam Schumach on Background Investigations Incident" (https://www.opm.gov/news/releases/2015/09/cyber-statement-923/).

*21 IPA, JPCERT/CC, "Alert 'Perform regular inspections to prepare for cyber attacks on websites'" (http://www.jpcert.or.jp/pr/2015/pr150003.html) (in Japanese).

August Incidents



V **5th: A number of vulnerabilities that could allow sites to be compromised, including XSS vulnerabilities, were discovered and fixed in the WordPress CMS application.**
"WordPress 4.2.4 Security and Maintenance Release" (https://wordpress.org/news/2015/08/wordpress-4-2-4-security-and-maintenance-release/).

O **5th: IPA published a report on the activities of the Cyber Rescue and Advice Team against targeted attack of Japan (J-CRAT), which was established to prevent the damages of targeted cyber attacks from escalating by supporting the mitigation of damage and blocking the chain of attacks.**
"Cyber Rescue and Advice Team against targeted attack of Japan (J-CRAT) activity report" (http://www.ipa.go.jp/files/000047193.pdf) (in Japanese).

S **6th: ICANN announced they had reset passwords due to the potential leak of the names, email addresses, and encrypted passwords of users registered to their website.**
"Reset ICANN.org Website Login Password" (https://www.icann.org/news/announcement-2015-08-05-en).

V **7th: A vulnerability (Certifi-gate) was disclosed in the authentication function of the mobile Remote Support Tools (mRST) installed in many Android devices, potentially allowing access to user data through the use of malicious applications.**
See the following Check Point blog post for more details. "Certifi-gate: Hundreds of Millions of Android Devices Could Be Pwned" (http://blog.checkpoint.com/2015/08/06/certifigate/).

V **12th: Microsoft published their Security Bulletin Summary for August 2015, and released a total of 14 updates, including four critical updates for MS15-079, MS15-080, MS15-081 and MS15-091, as well as 10 important updates.**
"Microsoft Security Bulletin Summary for August 2015" (https://technet.microsoft.com/library/security/ms15-aug).

V **12th: A number of vulnerabilities in Adobe Flash Player that could allow arbitrary code execution were discovered and fixed.**
"APSB15-19: Security updates available for Adobe Flash Player" (https://helpx.adobe.com/security/products/flash-player/apsb15-19.html).

S **12th: Cisco issued an alert due to confirmation of an attack that accesses IOS devices with administrator privileges and installs malicious ROMMON images.**
"Evolution in Attacks Against Cisco IOS Software Platforms" (http://tools.cisco.com/security/center/viewAlert.x?alertId=40411).

V **14th: Apple released an update that included fixes for a number of vulnerabilities in OS X.**
"About the security content of OS X Yosemite v10.10.5 and Security Update 2015-006" (https://support.apple.com/en-us/HT205031).

V **17th: An Italian security researcher disclosed a number of vulnerabilities in OS X without any fix available, along with PoC.**
These vulnerabilities were fixed along with others on October 1 with "About the security content of OS X El Capitan v10.11" (https://support.apple.com/en-us/HT205267).

V **18th: Actions such as the release of fixes were taken when it was discovered that old wireless LAN routers could be used as stepping stones in SSDP reflector attacks and exploited in DDoS attacks. As support has finished for one of the affected products, there have been calls to cease use of it.**
JVN, "JVN#17964918 Multiple I-O DATA LAN routers vulnerable in UPnP functionality" (http://jvn.jp/en/jp/JVN17964918/).

V **19th: Microsoft released a fix due to the discovery of a vulnerability (CVE-2015-2502) that could allow arbitrary code execution via the viewing of a specially-crafted website in Internet Explorer.**
"Microsoft Security Bulletin MS15-093 - Critical: Security Update for Internet Explorer (3088903)" (https://technet.microsoft.com/library/security/ms15-065).

O **20th: Verification reports were published by the Japan Pension Service and related government agencies regarding the leak of personal information from the Japan Pension Service in June.**
See the following for details of each report. National center of Incident readiness and Strategy for Cybersecurity, "Report on our investigation to determine the cause of personal information leaks at the Japan Pension Service" (http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf) (in Japanese). Japan Pension Service, "Report on our findings regarding the information leak caused by unauthorized access" (http://www.nenkin.go.jp/files/e7wRRjRfiKiN1.pdf) (in Japanese). Ministry of Health, Labour and Welfare (published August 21), "Verification committee report on information leaks caused by unauthorized access at the Japan Pension Service" (http://www.mhlw.go.jp/kinkyu/dl/houdouhappyou_150821-02.pdf) (in Japanese).

S **25th: U.S. company GitHub was targeted by a DDoS attack that interfered with their services.**
Details of this attack can be found on the following GitHub status page (https://status.github.com/messages/2015-08-25).

S **29th: The National Crime Agency (NCA) in the U.K. announced they had arrested or were interviewing six minors suspected of carrying out DDoS attacks using Lizard Stresser.**
National Crime Agency (NCA), "Operation Vivarium targets users of Lizard Squad's website attack tool" (http://www.nationalcrimeagency.gov.uk/news/691-operation-vivarium-targets-users-of-lizard-squad-s-website-attack-tool).

*Dates are in Japan Standard Time

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

■ Attacks Based on Political and Social Situation and Historical Context

During this period each year there are incidents related to historical dates in the Pacific War, as well as Takeshima and the Senkaku Islands. We stayed vigilant, as this year it was expected that the websites of a number of government agencies and private-sector businesses in Japan would once again be subject to defacement through compromise via SQL injection or unauthorized access, or targeted in DDoS attacks, in relation to these sensitive issues. A few more DDoS attacks than usual were observed, but no large-scale attacks were confirmed, and the scale and number of attacks decreased compared to the same period in previous years.

■ Government Agency Initiatives

Government agency initiatives with regard to security measures included the cabinet's approval of a new Cyber Security Strategy that determines the basic direction for cyber security policy. This strategy indicates the basic course of direction for policy in the next three years, taking into consideration the Tokyo 2020 Olympic and Paralympic Games. In light of the information leak that occurred at the Japan Pension Service in June, cyber security has been reinforced at all government agencies. For this reason, the strategy placed new emphasis on bolstering overall measures, including enhancements to the functions of the National center of Incident readiness and Strategy for Cybersecurity (NISC), and moves to monitor independent administrative corporations and special government-affiliated corporations that carry out public work alongside government ministries. After approval of the Cyber Security Strategy, the first annual plan based on it, Cyber Security 2015, was determined by the Cyber Security Strategic Headquarters*[22].

Verification reports regarding the leak of personal information that took place at the Japan Pension Service in June were published by NISC and the Ministry of Health, Labour and Welfare in August. As a result, the Cyber Security Strategic Headquarters issued a recommendation to the Ministry of Health, Labour and Welfare that monitoring of the Japan Pension Service be strengthened, and the roles and responsibilities of relevant departments at the ministry be clarified, based on Article 27 Item 3 of the Basic Act on Cybersecurity. It was also recommended that emergency procedures be put in place for when incidents occur.

In September, amendments to the "Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (My Number Act)" and "Act on the Protection of Personal Information" both passed the Lower House. The My Number Act was revised to expand the scope of use for the My Number system in areas such as finance and medicine. The My Number Act was enacted in October, and the Specific Personal Information Protection Commission published guidelines covering areas such as the response to leaks of specific personal information in anticipation of full scale operation, such as the issue of personal number cards that is set to start from January 2016*[23]. The Act on the Protection of Personal Information clarified the definition of personal information, and laid out laws regarding the handling of anonymous information processed to prevent personal information from being restored. It also established a new Personal Information Protection Committee with the authority to monitor and supervise the handling of personal information as a third party organization*[23].

In September, the "Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business" of the Ministry of Internal Affairs and Communications also produced its second report. In this report, the issuing of alerts to users of malware-infected devices and the blocking of communications with C&C servers, etc., were arranged. Consequently, the amendment of guidelines*[24] to apply the workshop's findings to the practical operations of telecommunications carriers was discussed at meetings such as the Council for the Stable Operation of the Internet.

■ Other

In July, the Italian security firm Hacking Team was attacked, resulting in the leak of a massive 400 GB of internal documents. The official Twitter account of the company was also taken over, and used to disseminate the stolen documents. This firm had been selling monitoring tools for devices such as PCs and smartphones to government and law enforcement agencies in a number of

*[22] National center of Incident readiness and Strategy for Cybersecurity (NISC), "5th assembly of the Cyber Security Strategic Headquarters (held on a rotating basis) (September 25, 2015)" (http://www.nisc.go.jp/conference/cs/index.html#cs05) (in Japanese).

*[23] See the following Specific Personal Information Protection Commission website for more information on the laws and guidelines regarding the My Number system (http://www.ppc.go.jp/en/).

*[24] "Guidelines for Dealing with High Volume Communications and Privacy at Telecommunications Carriers (Third Edition)" (http://www.soumu.go.jp/main_content/000362139.pdf) (in Japanese).

September Incidents

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

S **1st: The National Crime Agency (NCA) in the U.K. was targeted by DDoS attacks instigated by Lizard Squad, temporarily rendering their site inaccessible. This is thought to have been to avenge the arrest of Lizard Stresser users by the NCA in August.**

V **3rd: A number of vulnerabilities in the DNSSEC RDATA processing of the BIND9 that could allow DoS attacks from outside were discovered and fixed.**
Internet Systems Consortium, "CVE-2015-5986: An incorrect boundary check can trigger a REQUIRE assertion failure in openpgpkey_61.c" (https://kb.isc.org/article/AA-01291).

O **4th: A cabinet decision was made regarding the Cyber Security Strategy, which clarifies national policy towards cyberspace internally and externally, and indicates the basic direction for the next three years leading up to the Tokyo 2020 Olympic and Paralympic Games.**
National center of Incident readiness and Strategy for Cybersecurity (NISC), "Regarding Cyber Security Strategy" (http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf) (in Japanese).

S **5th: The official website of the town of Taiji in Wakayama Prefecture was targeted by DoS attacks carried out by Anonymous in protest against the drive hunting of dolphins and small whales, rendering it temporarily inaccessible (OpKillingBay).**

V **9th: A number of vulnerabilities in Adobe Shockwave Player that could allow arbitrary code execution were discovered and fixed.**
"APSB15-22: Security update available for Adobe Shockwave Player" (https://helpx.adobe.com/security/products/shockwave/apsb15-22.html).

V **9th: Microsoft published their Security Bulletin Summary for September 2015, and released a total of 12 updates, including five critical updates such as MS15-094, MS15-095, and MS15-099, as well as seven important updates.**
"Microsoft Security Bulletin Summary for September 2015" (https://technet.microsoft.com/library/security/ms15-sep).

O **9th: The Ministry of Internal Affairs and Communications published the "Second Report of the Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business," which evaluates suitable measures against cyber attacks in the field of telecommunications to enable telecommunications carriers to carry out new countermeasures and initiatives, while giving consideration to the secrecy of communications.**
"'Second Report of the Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business' and Results of Request for Public Comment Published (Ministry of Internal Affairs and Communications)" (http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000100.html) (in Japanese).

O **11th: The director of the Cyber Security Strategic Headquarters issued recommendations to the Minister of Health, Labour and Welfare based on Article 27 Item 3 of the Basic Act on Cyber Security taking into account the results of investigations into the leak of personal information from the Japan Pension Service. These recommendations asked for the establishment of a system for ensuring information security and handling information security issues, as well as the implementation of technological countermeasures, education and training for staff, and the evaluation and reporting of results.**
National center of Incident readiness and Strategy for Cybersecurity (NISC), "Recommendations based on Article 27 Item 3 of the Basic Act on Cyber Security" (http://www.nisc.go.jp/press/pdf/kankoku20150911_press.pdf) (in Japanese).

V **16th: A number of vulnerabilities that could allow sites to be compromised, including XSS vulnerabilities, were discovered and fixed in the WordPress CMS application.**
"WordPress 4.3.1 Security and Maintenance Release" (https://wordpress.org/news/2015/09/wordpress-4-3-1/).

P **18th: Attacks often occur around this day each year for historical reasons. However, although there were small-scale attacks this year, no organized attacks were observed.**

V **23rd: A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination or arbitrary code execution were discovered and fixed.**
"Security updates available for Adobe Flash Player" (http://helpx.adobe.com/security/products/flash-player/apsb15-23.html).

O **25th: The American Registry for Internet Numbers (ARIN), which manages Internet addresses in North America, announced that it had exhausted its stock of IPv4 addresses to allocate. In the future allocations will be made based on a waiting list.**
See "ARIN IPv4 Free Pool Reaches Zero" (https://www.arin.net/announcements/2015/20150924.html) for more information.

O **25th: An assembly of the Cyber Security Strategic Headquarters was held, and the Cyber Security 2015 annual plan based on the Cyber Security Strategy was determined.**
"5th assembly of the Cyber Security Strategic Headquarters (held on a rotating basis) (September 25, 2015)" (http://www.nisc.go.jp/conference/cs/index.html#cs05) (in Japanese).

O **30th: The National Police Agency published its "Report on Cyberspace Threats for the First Half of 2015," which gave an overview of trends in cybercrime for the first half of 2015.**
"Report on Cyberspace Threats for the First Half of 2015" (http://www.npa.go.jp/kanbou/cybersecurity/H27_kami_jousei.pdf) (in Japanese).

*Dates are in Japan Standard Time

Legend **V** Vulnerabilities **S** Security Incidents **P** Political and Social Situation **H** History **O** Other countries. The stolen information was also made available over BitTorrent, and because it contained customer lists and email content from the company, it came to light that many nations and intelligence agencies around the world were customers, including those in Asia, Europe, North America, South America, and Africa. A number of vulnerabilities in Adobe Systems' Flash Player and Microsoft's Windows[25] that had no fix available were also found via the leaked internal documents, so measures were taken to fix these vulnerabilities.

The email address for responding to support queries on a site related to the Cabinet Office was hijacked by an unknown party, leading to 20,000 spam messages being sent externally without authorization. In this incident, it has been identified that a contractor may have been using a short password that was easy to guess.

In September, Mandiant and FireEye announced they had discovered Cisco brand router products with altered firmware installed[26]. It is thought this was not due to vulnerabilities, but instead caused by malware installed on routers left with default authentication settings, or devices that had been managed improperly. Cisco issued an alert regarding these attacks in August, but investigations later published by research groups at academic organizations such as the University of Michigan indicated that infections were spreading, with 79 cases discovered in 19 countries[27].

Also in September, there was an incident in which an EV-SSL certificate for a Google domain was issued without authorization, but it is thought this certificate was mistakenly issued for internal testing. Google has registered revocation information for this certificate and revoked it[28].

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 July 1 and September 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.

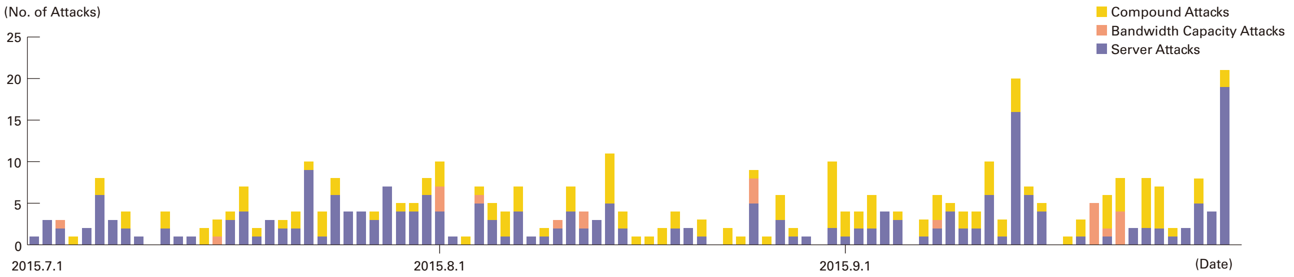


Figure 2: Trends in DDoS Attacks

[25] "Microsoft Security Bulletin MS15-078 - Critical: Vulnerability in Microsoft Font Driver Could Allow Remote Code Execution (3079904)" (https://technet.microsoft.com/en-us/library/security/ms15-078.aspx).

[26] See the following FireEye blog posts for more information about this attack. "SYNful Knock - A Cisco router implant - Part I" (https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html), "SYNful Knock - A Cisco router implant - Part II" (https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis0.html).

[27] ZMap, "In Search of SYNful Routers" (https://zmap.io/synful/).

[28] Google Online Security Blog, "Improved Digital Certificate Security" (https://googleonlinesecurity.blogspot.jp/2015/09/improved-digital-certificate-security.html).

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 on bandwidth capacity*[29], attacks on servers*[30], 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 400 DDoS attacks. This averages to 4.35 attacks per day, indicating an increase in the average daily number of attacks compared to our prior report. Server attacks accounted for 59.3% of all incidents, while compound attacks accounted for 34.9%, and bandwidth capacity attacks 5.8%. The largest attack observed during the period under study was classified as a compound attack, and resulted in 4.5 Gbps of bandwidth using up to 289,000 pps packets.

Of all attacks, 81.5% ended within 30 minutes of commencement, 17.8% lasted between 30 minutes and 24 hours, and 0.7% lasted over 24 hours. The longest sustained attack for this period was a compound attack that lasted for two days, 22 hours, and 35 minutes (70 hours and 35 minutes).

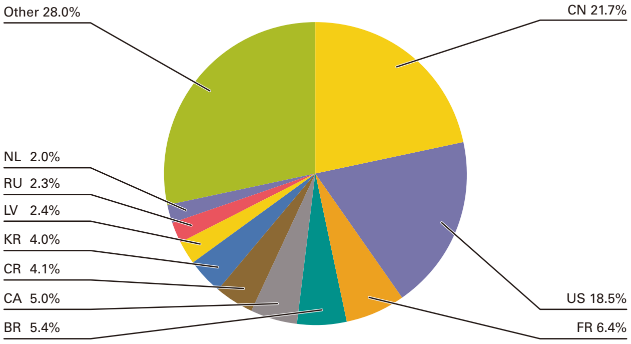


Figure 3: DDoS Attack Targets by Country According to Backscatter Observations

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*[31] and botnet*[32] usage as the method for conducting DDoS attacks.

Backscatter Observations

Next we present our observations of DDoS attack backscatter using the honeypots*[33] set up by the MITF, a malware activity observation project operated by IIJ*[34]. By monitoring backscatter it is possible to detect some of the DDoS attacks occurring on external networks as a third party without any interposition.

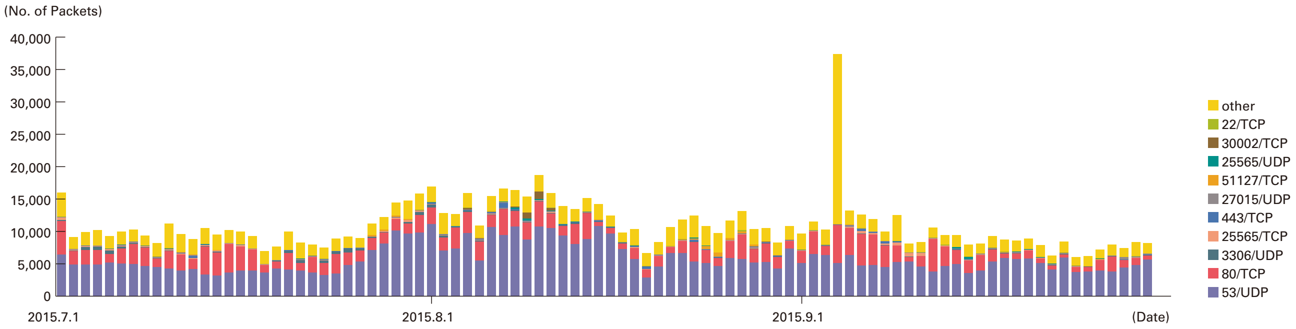


Figure 4: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)

*29 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.

*30 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.

*31 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.

*32 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.

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

*34 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."

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

The port most commonly targeted by the DDoS attacks observed was the 53/UDP port used for DNS, accounting for 53.2% of the total. This was followed by 80/TCP used for Web services at 20.6%, so the top two ports accounted for 73.8% of the total. Attacks were also observed on 443/TCP used for HTTPS, 22/TCP used for SSH, and 25565/TCP and 27015/UDP that are sometimes used for game servers, as well as 3306/UDP and 51127/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 remained mostly unchanged at around 5,800 compared to around 5,600 in the previous survey period, 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 21.7%. The United States and France followed at 18.5% and 6.4%, respectively.

Regarding particularly large numbers of backscatter packets observed by port, there were attacks on the Web servers (80/TCP and 443/TCP) of a U.S. hosting provider on July 1, and attacks on a number of servers of a hosting provider in Canada between July 13 and July 17. On August 7 there were attacks on game-related sites in France and Germany, and between September 4 and September 10 attacks targeting a number of servers of a U.S. CDN provider were observed. Attacks on other ports included those targeting 22/TCP, 8080/TCP, and 22/UDP on a server of a hosting provider in Canada between August 21 and August 27. We also observed attacks targeting 25565/TCP on a game server in France between September 5 and September 11. On September 4, a large number of attacks were also observed targeting a range of ports on a specific server in Latvia.

Notable DDoS attacks during the current survey period that were detected via IIJ's observations of backscatter included attacks on the servers of an instant messaging service provider based in Germany between July 10 and July 12, and attacks on the site for the Royal Canadian Mounted Police on July 18. Attacks were also observed targeting a site related to a right-wing organization in Ukraine on August 18, and targeting GitHub on August 25.

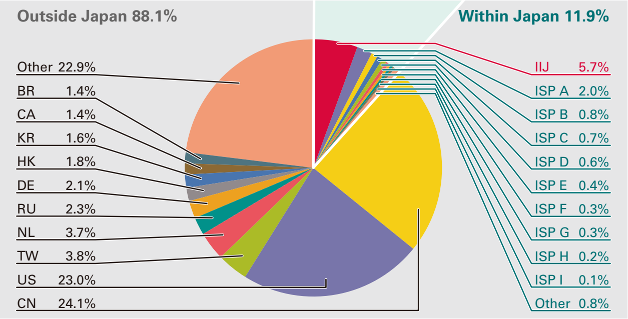


Figure 5: Sender Distribution (by Country, Entire Period under Study)

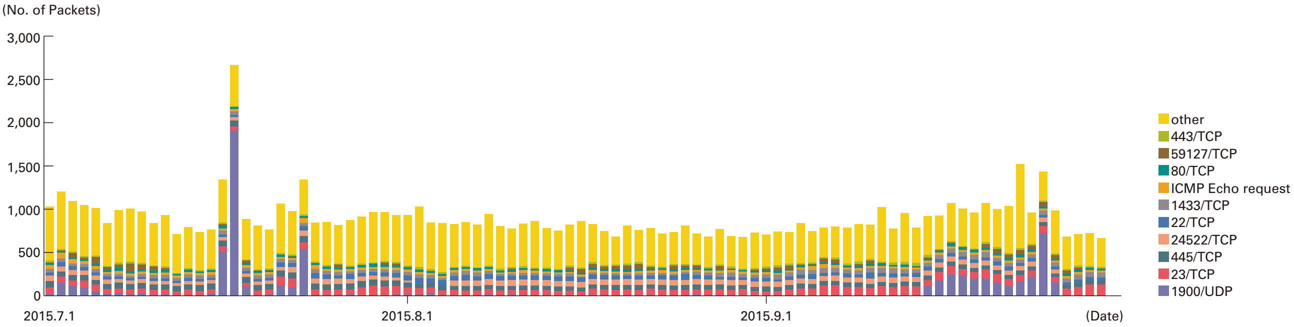


Figure 6: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the MITF*35, a malware activity observation project operated by IIJ. The MITF uses honeypots*36 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 between July 1 and September 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 targeted 1900/UDP used for the UPnP SSDP protocol, 23/TCP used for TELNET, 22/TCP used for SSH, 445/TCP used by Microsoft OSes, 1433/TCP used by Microsoft's SQL Server, or 80/TCP and 443/TCP used by Web servers.

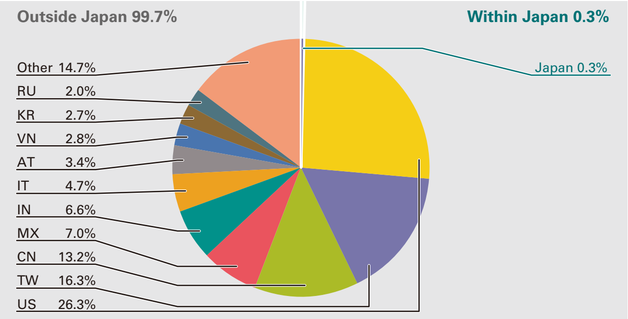


Figure 7: Distribution of Acquired Specimens by Source (by Country, Entire Period under Study, Excluding Conficker)

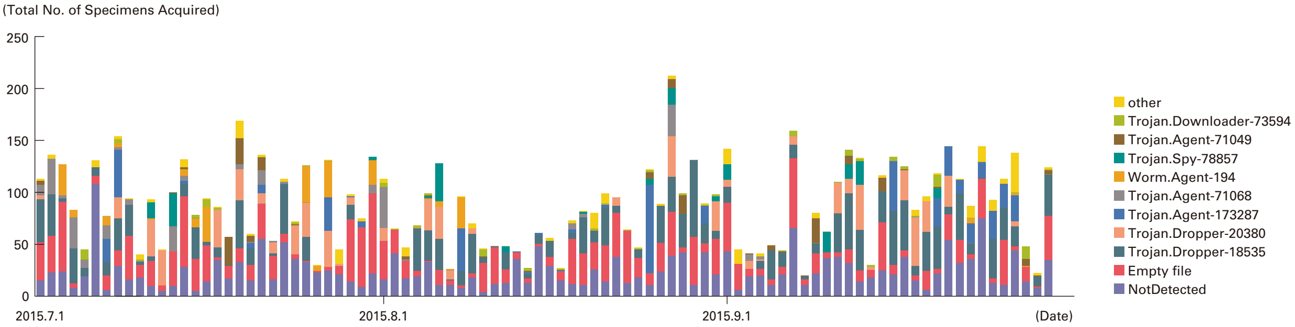


Figure 8: Trends in the Total Number of Malware Specimens Acquired (Excluding Conficker)

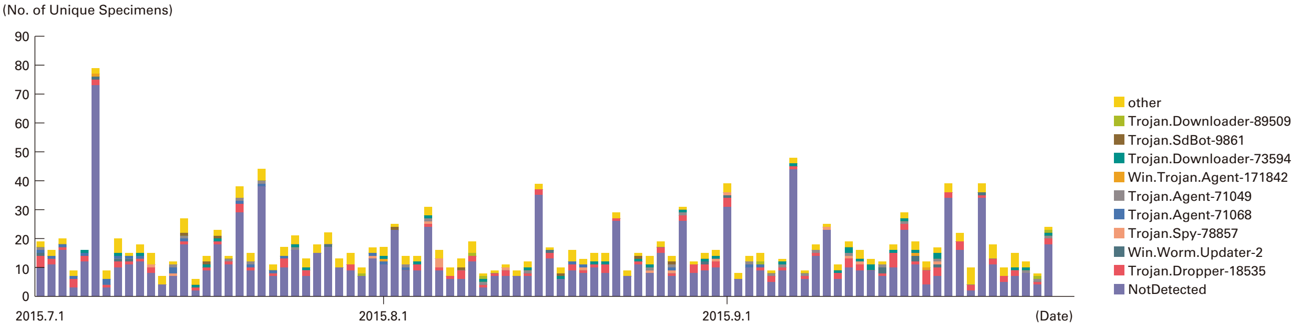


Figure 9: Trends in the Number of Unique Specimens (Excluding Conficker)

*35 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.

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

The 1900/UDP SSDP protocol spikes up in numbers intermittently. For example, we received SSDP search requests from IP addresses allocated to the United States between July 16 and July 17, from the Netherlands on July 23, and from addresses allocated to countries such as the United States, Australia, and Canada between mid-September and late September. These communications are thought to have been searching for devices that could be used in DDoS attacks using SSDP reflectors.

■ 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*[37], while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*[38]. Specimens are also identified using anti-virus software, and a breakdown of the top 10 variants is displayed color coded by malware name. As with our previous reports, 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, 89 specimens were acquired per day during the period under study, representing 19 different malware. After investigating the undetected specimens more closely, they included worms observed from IP addresses allocated to countries such as China, Taiwan, Austria, the United States, and Thailand. A bot that uses IRC as a C&C server*[39] was also observed in Taiwan*[40].

About 53% 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.

Under the MITF's independent analysis, during the current period under observation 84.6% of malware specimens acquired were worms, 6.4% were bots, and 9.0% were downloaders. In addition, the MITF confirmed the presence of 102 botnet C&C servers and 7 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.

■ Conficker Activity

Including Conficker, an average of 27,935 specimens were acquired per day during the period covered by this report, representing 543 different malware. Although the number of infections from the United States increased in July, they subsequently dropped, continually rising and falling over short periods. Conficker accounted for 99.5% of the total specimens acquired, and 98.8% 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*[41], as of October 1, 2015, a total of 675,680 unique IP addresses are infected. This indicates a drop to about 21% of the 3.2 million PCs observed in November 2011, but it demonstrates that infections are still widespread.

*37 This indicates the malware acquired by honeypots.

*38 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.

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

*40 WORM_SDBOT.FJK (http://www.trendmicro.com/vinfo/us/threat-encyclopedia/archive/malware/worm_sdbot.fjk).

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

1.3.3 SQL Injection Attacks

Of the types of different Web server attacks, IIJ conducts ongoing surveys related to SQL injection attacks*42. 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 July 1 and September 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. Japan was the source for 28.2% of attacks observed, while the United States and China accounted for 28.1% and 20.3%, respectively, with other countries following in order. There was a dramatic increase in the number of SQL injection attacks against Web servers compared to the previous report. This is due to a rise in attacks from countries such as Japan and the United States.

During this period, attacks from multiple attack sources in China and Germany directed at specific targets took place on July 18. There were also attacks from sources in a comparatively wide range of countries, including the U.K., Germany, Turkey, and the United States, targeting other specific targets. On July 24, there were attacks from a specific attack source directed at a number of specific targets. Other attacks were also made from specific attack sources in the United States and the Netherlands directed at specific targets. On August 1, there were attacks from specific attack sources in China directed at specific targets. There were also attacks on other targets from specific attack sources in the United States. On September 17, there were attacks from specific attack sources in China directed at specific targets. These attacks are thought to have been attempts to find vulnerabilities on a Web server.

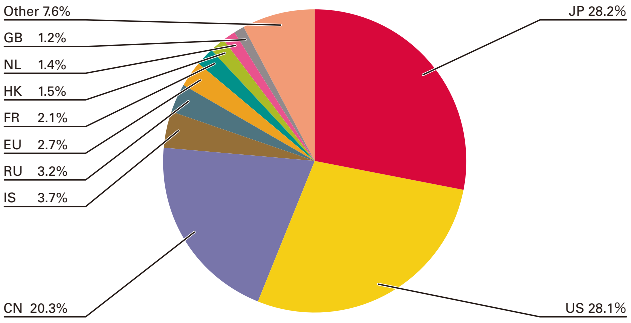


Figure 10: Distribution of SQL Injection Attacks by Source

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)*43.

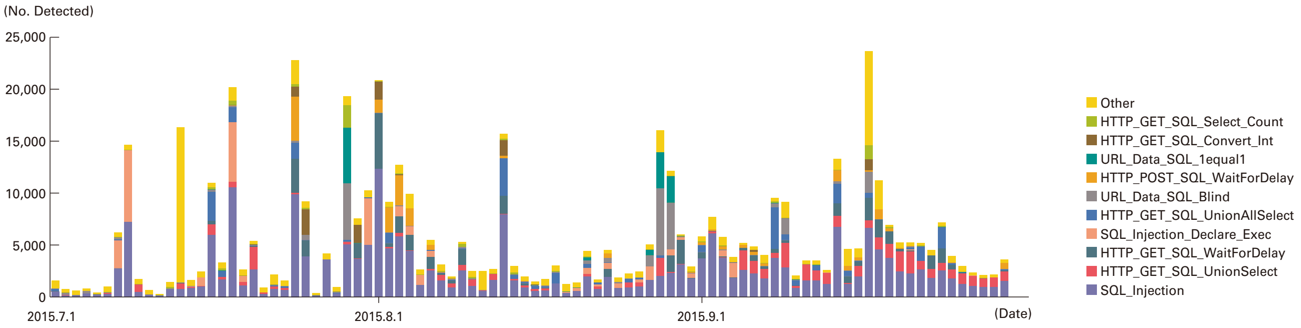


Figure 11: Trends in SQL Injection Attacks (by Day, by Attack Type)

*42 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.

*43 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.

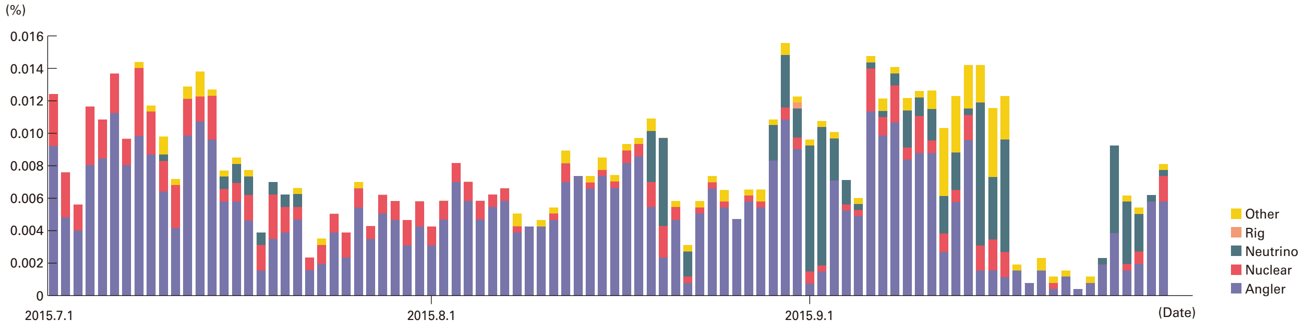
This Web crawler accesses hundreds of thousands of websites on a daily basis, with a focus on well-known and popular sites in Japan. We also add new target sites on a regular basis. In addition to this, we temporarily monitor websites that have seen short- term increases in access numbers. By surveying 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.

During the period of July to September, 2015, Angler spread like wildfire (Figure 12)[*44]. The total number of drive-by download attacks was almost 10 times the total number for April to June, 2015. Throughout this period, Angler accounted for the majority of attacks. However, in late August, some attackers that had up until then used Angler began using Neutrino. Since then, depending on the timing, attacks based on either the Angler or Neutrino Exploit Kit have been observed from the same altered website. Because the ratio of both varies each day, it appears as if the attackers are comparing multiple attack tools.

TeslaCrypt 2.0 made up the majority of the malware downloaded until early September, but after that it was replaced by CryptoWall 3.0, and TeslaCrypt 2.0 was no longer detected. In some cases observed, Bedep or Necurs were also downloaded in Angler and Neutrino attacks.

The number of attacks detected dropped sharply between September 18 and September 25. During this period, there were a number of cases in which the links on altered websites leading to exploit kits or their redirectors were deleted, or the next step leading from the redirector to the infector was not carried out. The attackers' intentions are not known, but the number of attacks detected subsequently increased again.

An extremely high number of drive-by download attacks continue to occur. In addition to altered websites, there have been many cases in which users were redirected to infectors via advertisement content displayed on a website (malvertising)[*45]. Website operators must take measures to prevent the alteration of Web content, and properly manage the mashup content provided by external third parties, such as advertisements and Web analytics services. We recommend that they stay aware of the security policies and reputations of content providers. It is also important for browser users and administrators to check for vulnerabilities in OSes and browser-related plug-ins, and carry out thorough countermeasures such as applying updates and enabling EMET.



*Covers several tens 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)

[*44] See "1.4.2 Angler Exploit Kit on the Rampage" in Vol.28 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol28_EN.pdf) for more information about our observations of the status and functions of Angler in July 2015.

[*45] See the Malwarebytes article "Large Malvertising Campaign Goes (Almost) Undetected" (https://blog.malwarebytes.org/malvertising-2/2015/09/large-malvertising-campaign-goes-almost-undetected/) for more information on malvertising during the same period.

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 will present information from the survey we have undertaken during this period regarding route hijacking and the latest status of TLS 1.3.

1.4.1 Route Hijacking

In January 2015, we discovered that a certain IPv4 address block managed by IIJ was being advertised to the Internet by a third party without authorization. IIJ dealt with the issue immediately, and carried out an investigation into the cause. Here we will discuss the current state of unauthorized route advertisement, and share some of what we learned from this incident.

■ The Inner Workings of Route Control

IP addresses are used to identify communication devices and point to destinations when communicating over the Internet. Of course, communications would not go well if IP addresses were to overlap, so to ensure each is unique, Internet Registries (IR) with a hierarchical management structure handle the allocation of IP addresses on the Internet. In Japan, IP addresses are usually allocated by applying to APNIC, the Regional IR (RIR) for the Asia-Pacific region, or JPNIC, Japan's National IR (NIR).

While organizations such as APNIC and JPNIC are responsible for IP address allocation and the associated management of registry information, matters such as ensuring the reachability of an IP address are the role of the party to which the address is allocated. To ensure reachability on the Internet, it is necessary to notify other networks of the details of the IP address block used. Currently, a routing protocol called BGP is the standard method used for routing control between networks, so each network uses BGP to generate information on the IP address block it is using, and notify other networks. This is known as route advertisement. Other networks receiving this route advertisement then forward IP packets bound for that IP address block to the network that advertised that route. Each network actually has its own BGP routing policy, and when route advertisements with different routes from the same address are received, only the route selected by the router as the optimal one based on priority level is used for packet forwarding.

BGP route advertisement itself is actually an easy process that simply involves adding a few lines of commands to the router, and based on the specifications anyone can advertise any route. The routing information advertised is also used as valid until revoked by the network that carried out route advertisement. In other words, incorrectly advertised routing information is instantly broadcast to the entire world, and remains in effect until the settings are explicitly canceled. Consequently, when carrying out new route advertisement, it is crucial to avoid configuration and confirmation errors. However, with the spread of the Internet a range of networks around the world now exchange routes via BGP, so it is inevitably possible for errors to occur at some point. Additionally, when a router exchanging routes via BGP is hijacked by someone with malicious intent, improper route advertisement may be carried out willfully. It is important to check that the routers on each network are being operated appropriately, by applying access control, performing monitoring, and carrying out regular inspections of their settings.

■ Routing Security

There are a number of ways to reduce configuration errors and mitigate the impact of false route advertisement. First, when advertising routes, the validity of advertised routes for that IP address block is checked. IR such as APNIC and JPNIC publish registry information for the IP addresses they allocate via whois, so it is possible to refer to this to check that there are no discrepancies between the allocated organization and the IP address block. It is also effective to implement route filters at network interconnection points to prevent the propagation of false routing information. In particular, it is possible to limit the scope of impact that false routing information has by applying strict inbound route filters to transit networks that relay routing information. For this reason, organizations that provide transit services in many cases operate by having customers notify them of IP address block information scheduled to be advertised in advance, and updating the route filter based on this. Even so, cases of false route advertisement continue to happen in actual practice. This is sometimes referred to as "route hijacking," but in many reported cases the route advertisement was corrected immediately after being advertised, so it is thought that most are the result of unintended configuration errors. For this reason, we believe the term "unauthorized route advertisement" is more appropriate when referring to the phenomenon as a whole.

These cases of unauthorized route advertisement can also affect reachability, so it is necessary to detect them when they occur. A variety of detection-related initiatives are being carried out around the world, and in Japan Telecom-ISAC Japan and JPNIC have formed a partnership to operate the “Keiro-Bugyo” route hijacking detection system. Keiro-Bugyo utilizes the route objects registered to the JPIRR Internet Routing Registry (IRR) operated by JPNIC as standards to determine correct routing, comparing this data with BGP routing information submitted to the system by ISPs in Japan to detect anomalous routes. Routes that are advertised from a source other than the one registered to the route object are treated as anomalous, so this system is useful for detecting anomalous routes due to configuration errors. Additionally, because routing information is obtained from ISPs in Japan, it is possible to predict the impact within Japan to a certain extent. IIJ has participated in the operation of this system since it was introduced, and we have been committed to activities that further improve detection rates. IIJ also uses the system to monitor routes itself, and in the past we have taken action after receiving an alert from Keiro-Bugyo when routes advertised by IIJ were also advertised by other networks.

Classifying false route advertisements using a detection system is a difficult task. For example, erroneously registered route objects are also detected as anomalies by Keiro-Bugyo. As external parties cannot know the usage intended by the administrator of an IP address block, it is hard to confirm whether this configuration is legitimate or not, so they can only be classed as “suspected” route hijackings. It is also rare to receive a report on the cause from the party the false route advertisement originated from. In cases shared by Telecom-ISAC Japan, inquiries to networks where a route advertisement originated were also simply answered with “we fixed it,” so there were many times when it was unclear whether incidents were caused by a configuration error on-site, or some other reason. The incidents we discuss here that IIJ responded to are valuable cases of “route hijacking” where our investigations into the cause clearly identified that the perpetrator had malicious intent.

■ Overview of Route Hijacking Incidents

On February 4, 2015, an email message was posted to a mailing list for the JApan Network Operators’ Group (JANOG). It indicated that a /16 IPv4 address block managed by IIJ was advertised by another network, and included in the Spamhaus Block List. After seeing this, we took action immediately. As route advertising for the block in question was in fact being performed by an ISP in the United States, our first aim was to take back the route and stop it from the source it was being advertised from. Because routing information for a smaller address block is given a higher priority (more specific routes) when it comes to IP route control, we advertised more specific routing information as a temporary measure so that route advertisement from IIJ was given priority on other networks. At the same time, we looked up the contact information for the corresponding ISP in the United States, and got in touch with them. ISPs have a range of different points of contact, such as those for business inquiries, and support desks for each service, so unless you direct your inquiries appropriately it could take time to receive a response, or you may be ignored for contacting an unrelated department. For routing issues such as these, it is necessary to identify the network operations center (NOC) of the organization in question, so we searched using whois and the ISP’s website, and got in touch with the point of contact that seemed most likely to apply.

After sending the details to the corresponding ISP by email, we also contacted them by phone straight away to confirm they had received the email and ask for a response. Because many ISPs in the U.S. have implemented a ticket system that manages the progress of tasks, we also asked for a ticket number to be issued. We were told that the ticket number would be sent by email, so we waited for a reply, but we had not received a response over 24 hours later. For that reason, we called them once again, and requested that a ticket be issued then and there. As a result we were finally assigned a ticket number that we could use to track progress. Because a different staff member took the call than the one we had spoken to before, we once again asked them to confirm the whois information on the spot, to have them acknowledge that our request was legitimate. According to the information from the ISP, they began advertising the IPv4 address block at issue at the request of a customer. They agreed to contact that customer and cease advertising the route within 24 hours, even if they got no reply. As a result, after making contact on the afternoon of February 4, 2015, the corresponding route advertisement ceased three days later, in the early hours of February 7, 2015. Because this IPv4 address block was included in the Spamhaus Block List, we requested that it be removed after the false route advertisement ended, and the following day it was deleted from the list.

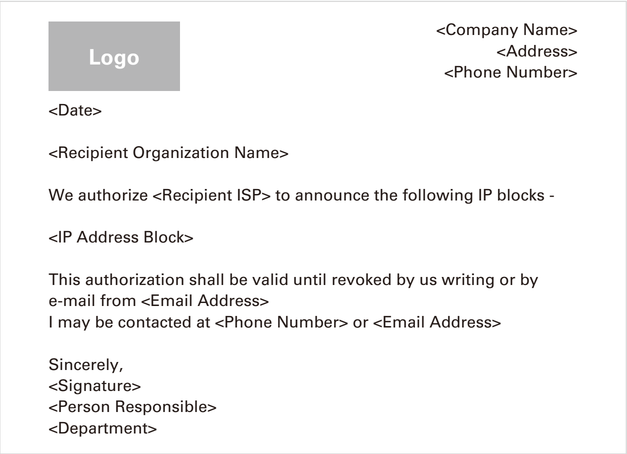
Looking at the history of routing information in IIJ's possession, this false routing information began to be advertised on January 5, 2015, but IIJ did not notice until the details were posted to JANOG. This IP address block actually came to be managed by IIJ based on IPv4 address transfer procedures, and at the time we were retaining it for future use without advertising the routes. While the whois information registered to JPNIC was of course up to date, in part due to the routes not being advertised, they were not registered in the route database of JPIRR, etc., and were not subject to monitoring by the aforementioned Keiro-Bugyo system. Consequently, we were not aware when false route advertisement occurred. As a result of this incident, we reappraised all of the IP address blocks under our management, and began registering them to IRR such as JPIRR and carrying out route advertising. This means all IP address blocks that IIJ manages are currently monitored by Keiro-Bugyo.

To prevent the issue from reoccurring, we asked the U.S. ISP that had been the source of the false route advertising to provide us with information related to the origin of the route advertising. After tireless negotiations, we were sent a surprising document on February 27, 2015, about three weeks after they stopped route advertising. Figure 13 is a document known as a Letter of Authority (LoA), which is submitted when a customer requests that an ISP advertises an IP address block of their own.

Because a formal document from an organization is required, letterhead format is used, with the company's logo and contact details listed at the top of the document. This simply contains a statement authorizing the ISP to carry out route advertisement, the IP address block to be used, the contact details and signature of the responsible person, and the date. Looking at the details that were submitted in the document, it was presented as being from the organization that had managed the IPv4 address block before it was transferred. That said, the organization name and contact details were slightly different from those we were familiar with.

To confirm, we brought the document to the organization that had managed the corresponding IPv4 address block before the IPv4 addresses were transferred, and had them look over it. As it turns out, it was indeed a falsified document. They confirmed the company name listed did not exist, and that it was highly likely the logo and address of a related company had been used. It was also clarified that the phone number and responsible person were most likely reused from information previously registered to whois. They had no knowledge of the domain name for the email address specified under the contact details. The document was signed by the person formerly responsible, but they confirmed that this signature did not match that for the staff member in question. The perpetrator appeared to have registered a new domain name that resembled the company name to use, and the whois information for the domain name matched the company name and staff member name on the LoA document.

Here we will present a timeline for these events, including some estimates (Figure 14). The domain name used as a cover on the LoA was registered on October 7, 2014, so it seems likely that the target was chosen before this date. We speculate that at this time an IPv4 address block without existing route advertisements or a specific point of contact was chosen so they could make use of it for as long as possible. Then, on October 7, they registered the domain name to be used as a cover based on the whois



Logo

<Company Name>
<Address>
<Phone Number>

<Date>

<Recipient Organization Name>

We authorize <Recipient ISP> to announce the following IP blocks -

<IP Address Block>

This authorization shall be valid until revoked by us writing or by e-mail from <Email Address>
I may be contacted at <Phone Number> or <Email Address>

Sincerely,
<Signature>
<Person Responsible>
<Department>

Figure 13: LoA Example

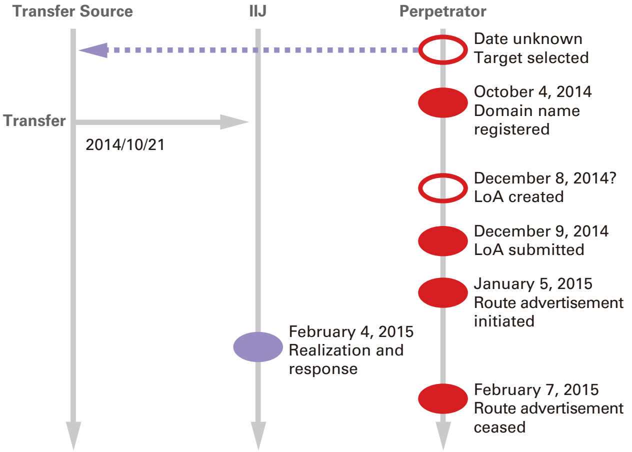


Figure 14: Timeline of the Incident

information of the target. After that, they would have had to organize a suitable server that could receive email. Subsequently, while the perpetrator was making preparations, something they did not foresee happened. Namely, the transfer of IPv4 addresses. From October 21, 2014, the IPv4 address block in question came under the management of IIJ. However, we believe it likely that the perpetrator was not aware of this. On December 9, 2014, they followed through with their preparations by submitting the LoA in PDF format to the U.S. ISP that eventually advertised the routes, under a name resembling the organization that managed the addresses prior to their transfer. As a result, the ISP advertised routes for the corresponding IPv4 address block from January 5, 2015, to February 7, 2015, when they were contacted by IIJ and ceased advertising.

Upon investigating details associated with this incident, we discovered that other suspicious incidents had occurred. On February 10, 2015, three days after advertisement of the IP address block ceased based on IIJ's request, the IP address block next in sequential IP address order began to be advertised by the same ISP. After investigating, we learned that this was done by the same perpetrator, using almost the same technique to have the route advertised. It seems that this incident was dealt with independently, and route advertisement ceased on May 16, 2015. The Internet was introduced to Japan at an early stage compared to other regions around the world, and in its early years there were organizations that were allocated comparatively large IP address blocks. Of these IP address blocks, those with incomplete whois information or inaccurate contact details, those being held in reserve, and those only used internally with routes not advertised over the Internet, are likely to be easy targets for false route advertising like the incident we are discussing here. For that reason, we recommend evaluation of the measures described below.

Let us consider what uses the perpetrator had in mind for the network. IIJ has actually not been able to ascertain the details of this incident. Thorough and exceedingly risky measures were employed, such as registering a fake domain name and producing fake documentation, so we think there was some kind of malicious intent. However, we have no evidence of what the network was used for, so we do not know what its purpose was. Our investigation into this incident is ongoing. Regarding other incidents, cases in which IP addresses were exploited to send spam have been reported. The SANOG community for the South Asian region has shared information about an incident in which the administrator of a certain network suddenly began receiving a torrent of spam complaints. After the administrator looked into the issue, they found that an IP address block had been subject to a temporary route hijacking, and apparently used to send large volumes of spam. Because route hijacking is sometimes discovered through complaint emails to administrators, it is important to maintain your point of contact and continue to deal with complaints.

■ Lessons Learned from the Incident, and Route Hijacking Measures

The false route advertising that took place in this incident could have been prevented if the ISP in question had screened the documentation properly. The JPNIC whois information had been changed to IIJ's contact details by the time the LoA arrived, meaning there were discrepancies in the documentation. On the other hand, whois searches require a certain amount of knowledge and technique. Because the IR that manage IP address registry information form a hierarchical structure, it is necessary to navigate your way back up as you search. Some whois clients can trace this automatically to a certain extent, but there are few regions with a NIR for each country, so most clients search and display results based on the RIR whois for each region, or in other words on the APNIC whois level in the Asia-Pacific region. The English portion of the information registered to JPNIC is also transferred to the APNIC whois and displayed there, but to decipher this correctly you need to know how each piece of information is being reflected. The management of blocks registered at the dawn of the Internet has been transferred to the regional RIR of registrants in the ERX project, and it recently became possible to transfer IPv4 addresses across regions, so this also makes it necessary to perform whois searches by tracing the path appropriately to gain the correct information.

Resource Public Key Infrastructure (RPKI) is a standardized format for registry information that is a little easier to use on computers than whois. This involves using digital certificates to describe the assignment or allocation of Internet number resources such as IP addresses. It is possible to issue digital certificates called resource certificates based on IR registry information, and you can use these to verify the assignment and allocation of IP addresses. Because digital certificates are utilized, you can also add digital signatures to documents. For example, by attaching a digital signature to an LoA using a resource certificate, and validating it on the recipient side, it is possible to check that the document is from the genuine administrator of the IP address block. They can also be used for route control. Currently, Origin Validation technology that validates the AS number of the origin of a route has been standardized, and progress is being made with its implementation on routers. The operator must learn about general public key cryptography technology such as PKI, but if run correctly this should serve as a very robust authentication infrastructure. We believe it will take some time for it to become widespread, but IIJ would like to contribute to the popularization of RPKI through validation and operation. Let us examine what measures can currently be taken when you are assigned or allocated IP addresses. Through this incident we have learned that the following two points are likely the keys to reducing the likelihood of being targeted and enabling ISPs to notice abnormalities when route advertising is requested.

1. Ensure that whois contact details are maintained
2. Advertise routes

Regarding whois information, we recommend that contact details be recorded as accurately as possible, including the organization name and address, phone number, and email address, so they can be used for identification when referred to. This whois information is also sometimes referenced to find contact details and lodge grievances, so it is necessary to be aware that these points of contact may end up processing complaints, and because it serves as a public window, they could end up receiving spam on a daily basis. Complaint emails sometimes have spam attached to them, but if you apply a simple learning or keyword match spam filter the complaints themselves may be detected as spam and not received, so caution must be exercised.

As for route advertisement, even when Internet reachability is not required, it is safer to advertise routes to indicate they are being operated properly. That said, when routes are advertised, IP packets destined for those IP address blocks will be taken in, meaning that IP packets used to probe for vulnerabilities or services that are operating will arrive. To avoid taking unnecessary risk and maintain the current environment to the extent possible, we recommend that you merely advertise routes, while discarding all packets destined for those IP address blocks. When already using some kind of Internet access service, that ISP may be able to take care of this if you ask them, and if necessary you would be welcome to discuss the issue with IIJ. When advertising routes, they will be subject to the Keiro-Bugyo monitoring service if the route objects are properly registered in the JPIRR routing information database. This increases the chances of detecting fraudulent route advertising at an early stage, so we recommend you look into doing this also.

It is likely that other route hijacking attempts such as the incident discussed here will continue to be made on the Internet. From our point of view, there are two main reasons for this. Firstly, because a range of organizations are investigating the sending of spam and hosting of malware, and building reputation databases on an IP address level, there is demand for new IP address blocks that can be exploited for any purpose. Secondly, the free pool of IPv4 addresses is running out around the world, gradually making it harder and harder to secure the required amount of IPv4 addresses through existing services. Due to these circumstances, we believe there is an ongoing risk of route hijacking taking place. Also, as mentioned before, the whois information for many IP address blocks in Japan that were allocated in the early days of the Internet has not been updated properly, making them ripe targets for hijacking. When an IP address block you manage is exploited via route hijacking, it may be added to block lists you aren't aware of, or given a low rating in a reputation database. This could affect communications in the future. You may also be caught having to handle complaints you have no knowledge of, so we recommend that suitable measures be taken.

■ Summary

Much like other security measures, it is important to approach route hijacking countermeasures from the perspective of increasing the cost to the attacker. We consider it crucial to prepare an environment that doesn't easily fall victim to route hijacking, and put in place a system for detecting and dealing with route hijacking swiftly when it does occur. To achieve this, it will be necessary to look into implementing a range of technological and operational initiatives. These include improving the reliability of IR registry information, and re-examining validation methods for IP addresses provided by customers through the utilization of RPKI. We also need to implement measures for preventing the distribution of false route information, such as the operation of strict route filters or route authentication via RPKI. Another key point is enhancing technology for detecting fraudulent routes through Keiro-Bugyo and other abnormal route detection mechanisms. Building cooperative and trusting relationships that enable the sharing of required information and coordinated responses between networks is another crucial factor. In addition to this, we would also like to build an environment that prevents the recurrence of route hijacking, while consulting with law enforcement agencies and other organizations. These initiatives will be carried out in cooperation with many others involved in Internet routing, and do not only concern IIJ, so we would like to share our knowledge with as many people as possible, and continue to perform tests, have discussions, and make improvements in the future.

1.4.2 The Latest Status of TLS 1.3

Due to the discovery of a string of different vulnerability types affecting the SSL (Secure Socket Layer) / TLS (Transport Layer Security) secure protocols implemented in a wide range of browsers, there have been calls for a fundamental solution. Consequently, all eyes are focused on TLS 1.3, the next version of the TLS protocol. In this report we will touch upon the issues and background of previous versions, and examine the current development of TLS 1.3.

■ The History of SSL/TLS

In 1995, SSL 2.0 was implemented in the Netscape Navigator browser of the day, in the same period as the Internet draft “draft-hickman-netscape-ssl” was published by Netscape Communications. SSL 3.0, which fixed a number of problems and also included some extensions, was subsequently used until recently. However, after the POODLE attack disclosed in October last year exposed fundamental flaws in SSL 3.0, SSL was no longer considered secure to use. Currently, it is recommended that neither SSL 2.0 nor SSL 3.0 be used[*46]. RFC for versions 1.0, 1.1, and 1.2 of TLS, the successor to SSL that was drawn up by the IETF, were released in 1999, 2006, and 2008, respectively[*47]. Details of the main changes in each version are discussed in the guidelines[*48] created by the CRYPTREC cryptographic technology evaluation project. To give an overview, an issue when using the CBC mode in TLS 1.0 that was widely exposed by attacks such as the BEAST attack was identified, and TLS 1.1 resolved this problem. In TLS 1.2 it became possible to use comparatively new cryptographic algorithms, such as GCM and CCM that are classified as authenticated encryption modes, and the SHA-2 families.

Table 1 summarizes the workarounds in each version[*49]. TLS 1.0 can be safely used by working around a number of issues in the specifications using server configuration or client implementations, and is currently the most widely used version. It is also possible to support TLS 1.1 and TLS 1.2 by using a new TLS library or cryptographic module, and users are able to use secure versions without any additional hassle by updating their browser to the latest version. However, this does not change the fact that there are no fundamental solutions to some issues. Revisions and discussions are still being carried out regarding TLS 1.3 at the time of writing, in response to calls for fundamental fixes to a variety of vulnerability types in SSL/TLS. We offer a technological explanation of the TLS 1.3 draft later in this article.

Table 1: Differences in Status Based on Variance in SSL/TLS Versions

Protocol	Version	Status	Workaround	Basis
SSL	2.0	Vulnerable	N/A	RFC6167
	3.0	Vulnerable	N/A	RFC7568 (POODLE attack)
TLS	1.0	Issues present but workarounds available (however, some issues have no workaround)	Do not use the renegotiation function	RFC5746
			Do not use the compression function	CRIME attack
			1 : n-1 splitting	BEAST attack
			Risk acceptance	Lucky-13 attack
	1.1	Issues present but workarounds available (however, some issues have no workaround)	Do not use the compression function	CRIME attack
			Risk acceptance	Lucky-13 attack
	1.2	Issues present but workarounds available	Do not use the compression function	CRIME attack
			Only use GCM or CCM block cipher modes	Lucky-13 attack
	1.3	(Under development to be secure)		

■ Overview and Roles of SSL/TLS

The functions of SSL/TLS are (1) encryption of communications, (2) ensuring the integrity of data, and (3) server authentication (as well as client authentication in some cases). Located at the session layer, it is possible to provide the abovementioned security functions under a range of application layer protocols, such as HTTP, SMTP, and POP, without the need to implement mechanisms to ensure security for each of them. Because it has the advantage of not being dependent on the protocols of the application layer, it has been implemented widely.

[*46] See “SSL and TLS: Theory and Practice” by Rolf Oppliger for more information on the history and background for the formulation of SSL/TLS. The reasons the use of SSL is not recommended are summarized in the following two RFC. “RFC 6176: Prohibiting Secure Sockets Layer (SSL) Version 2.0” (https://tools.ietf.org/html/rfc6176), “RFC 7568: Deprecating Secure Sockets Layer Version 3.0” (https://tools.ietf.org/html/7568).

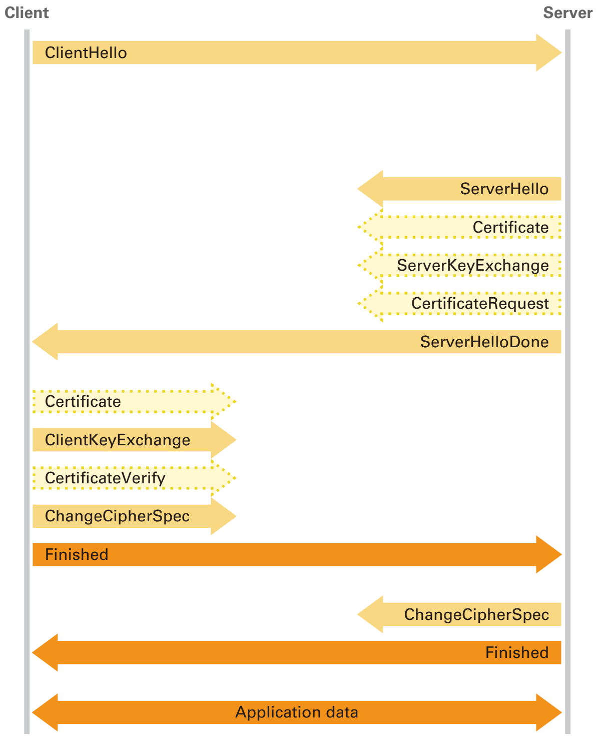
[*47] “RFC 2246: The TLS Protocol Version 1.0” (https://tools.ietf.org/html/2246), “RFC 4346: The Transport Layer Security (TLS) Protocol Version 1.1” (https://tools.ietf.org/html/4346), “RFC5246: The Transport Layer Security (TLS) Protocol Version 1.2” (https://tools.ietf.org/html/5246).

[*48] IPA, “Cryptography Configurations Guideline for SSL/TLS Websites (- Cryptographic Configurations Edition)” (http://www.ipa.go.jp/security/vuln/ssl_crypt_config.html) (in Japanese).

[*49] Recommended settings can be found in the aforementioned Cryptography Configurations Guideline, the Mozilla project’s “Security/Server Side TLS” (https://wiki.mozilla.org/Security/Server_Side_TLS), or “RFC 7525: Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)” (http://tools.ietf.org/html/rfc7525). “RFC 7457: Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS)” (https://tools.ietf.org/html/rfc7457) also contains an overview of attacks to date.

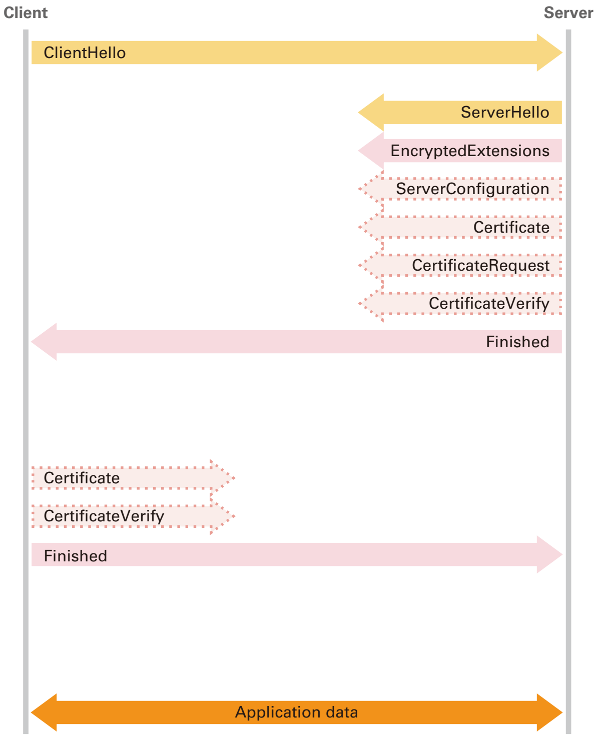
Figure 15 shows the message flow in TLS 1.2. Pre-processing called the Handshake message takes place before the encryption of application data, consisting of a four-way flow. A brief explanation of the role of the Handshake message is given below. (1) A list of acceptable cipher suites (combinations of cryptographic algorithms) is sent from the client (browser) to the server. (2) The server selects the cipher suite considered best from among these, and sends notification via a ServerHello message, while also returning information such as the X.509 certificate required for server authentication and the public key, etc. required for key exchange to the client. (3) Because the client receives the server's public key, it can send information that only the server can decrypt. Once the server receives and decrypts this, it shares the Master Secret that all forms of key data are based on. Next, after sending a CCS (ChangeCipherSpec) message that indicates encryption will be used from that point on, the encrypted Finished message is sent. The server decrypts this, and checks the MAC data (data that ensures the integrity of a message) contained within to confirm that the messages sent and received up to that point have not been altered. (4) Finally, the server also sends a CCS and the encrypted Finished message, and the receiving client performs decryption and checks the MAC data in the same way that the server did, establishing a framework for sending and receiving application data securely.

Through the use of public key cryptosystems, the keys used for data encryption are generated in such a way that they are only known to the client and server, providing an encryption function. The MAC data also covers all the plain text data before the Finished message, so this provides a system for detecting alterations somewhere along the communication path. In addition, it is possible to carry out server and client authentication by confirming that the other node has the private key that corresponds to the public key presented in the X.509 certificate.



In the diagram, messages bordered with a dotted line are optional, and orange messages indicate encryption has been carried out using key data derived from the Master Secret.

Figure 15: TLS 1.2 Message Flow



Only the "Message flow for full TLS Handshake" (also called 1-RTT) in the TLS 1.3 draft is shown in this figure. Discussions regarding the merge of CertificateRequest and CertificateVerify are ongoing, but ultimately it is likely they will be changed. Also note that some flows do not match this. In particular, for 0-RTT in which clients store EarlyDataIndication, a type of previously shared information, inside ClientHello for transmission, the flow differs greatly due to the fact that keys have already been shared. At IETF-94 it was proposed that client authentication be carried out after the Handshake, so even more variations are expected to appear. In the diagram, messages surrounded by a dotted line are optional, pink messages are encrypted with key data derived from the Ephemeral Secret, and orange messages are encrypted with key data derived from the Master Secret.

Figure 16: TLS 1.3 Message Flow

TLS 1.3

TLS 1.3[*50] is still being revised and discussed at the time of writing. This is not a comparison with the final specification, but compared with TLS 1.2 or earlier, rather drastic changes such as those below are expected to be adopted.

(1) Deprecation of compromised algorithms and block cipher modes.
(2) Simplification of the message flow and encryption of the Handshake message.
(3) Reorganization of pseudo-random number generation functions, and changes to the Master Secret calculation method and key derivation processes.

There are other changes besides those mentioned above, and it is clear that many improvements are being attempted. Engineers will be watching with interest to see how things develop. In Japan, events to review the latest draft have also been held led by CELLOS (Cryptographic protocol Evaluation toward Long-Lived Outstanding Society), and an effort has been made to send the results of these reviews to the TLS working group as feedback[*51].

Below, we give a brief overview of the changes listed above from a technological perspective.

(1) Deprecation of compromised algorithms and block cipher modes.

Cryptographic algorithms such as DES, MD5, and RC4 that are considered compromised will be deprecated[*52]. There are moves to deprecate RC4 in particular independently of TLS 1.3 development, with major browser vendors already announcing they will disable support for RC4 early in 2016[*53]. Of the SHA-1 and SHA-2 series of algorithms, SHA-224 will also be eliminated from use in signatures. However, as certificates using SHA-1 have not been completely eliminated from certificate chains that are traced to verify server certificates, talks aimed at finding a way to handle this are still ongoing. The CBC block cipher mode that led to attacks such as BEAST and POODLE will be deprecated, so only AEAD (Authenticated Encryption with Associated Data) will be used for symmetric key cryptography. The AEAD competition CAESAR[*54] has been held since 2013, and is currently in the Round-2 phase. The winner(s) are set to be determined by around the end of 2017. It is not clear whether the results of CAESAR will be applied to TLS 1.3, but in the current draft version the ChaCha20-Poly1305[*55] implementation of AEAD is listed as a mandatory algorithm alongside AES-GCM and AES-CCM[*56]. Other symmetric key cryptographic algorithms listed include South Korea's ARIA and Japan's Camellia[*57]. Going forward, it is expected that requests to list other algorithms will come flooding in, so the process by which the final selection will be made is expected to all come down to the details.

[*50] "The Transport Layer Security (TLS) Protocol Version 1.3" (https://tlswg.github.io/tls13-spec/), or "The Transport Layer Security (TLS) Protocol Version 1.3" (https://datatracker.ietf.org/doc/draft-ietf-tls-tls13/). At the time of writing, the latest edition of the draft is version 10.

[*51] At a study group held four times between June and September, comments on the draft revision-08 were summarized and published (https://www.cellos-consortium.org/studygroup/tls_1_3-draft_08_issues_rev1.pdf). These comments were also posted to the TLS working group mailing list (http://www.ietf.org/mail-archive/web/tls/current/msg17904.html). The current status of each can be reviewed on GitHub (https://github.com/tlswg/tls13-spec/search?q=CELLOS&type=Issues&utf8=%E2%9C%93).

[*52] DES was already deprecated in TLS 1.2. See "RFC 6151: Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms" (https://tools.ietf.org/html/6151) for more information on the deprecation of MD5. Similarly, see "RFC 7465: Prohibiting RC4 Cipher Suites" (https://tools.ietf.org/html/7465) for information on RC4.

[*53] The RC4 NOMORE Attack (https://www.rc4nomore.com/) was disclosed at USENIX security'15 this summer, serving to hasten moves to deprecate RC4. Actions from major browser vendors were as follows, "Ending support for the RC4 cipher in Microsoft Edge and Internet Explorer 11" (http://blogs.windows.com/msedgedev/2015/09/01/ending-support-for-the-rc4-cipher-in-microsoft-edge-and-internet-explorer-11/), "Deprecating the RC4 Cipher" (https://blog.mozilla.org/security/2015/09/11/deprecating-the-rc4-cipher/), "Intent to deprecate: RC4" (https://groups.google.com/a/chromium.org/forum/#!msg/security-dev/kVfCywocUO8/vgi_rQuhKgAJ)

[*54] Cryptographic competitions, "CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness" (http://competitions.cr.yp.to/caesar.html).

[*55] "RFC 7539: ChaCha20 and Poly1305 for IETF Protocols" (https://tools.ietf.org/html/rfc7539).

[*56] "RFC 5288: AES Galois Counter Mode (GCM) Cipher Suites for TLS" (https://tools.ietf.org/html/rfc5288), "RFC 6655: AES-CCM Cipher Suites for Transport Layer Security (TLS)" (https://tools.ietf.org/html/rfc6655).

[*57] "RFC 6209: Addition of the ARIA Cipher Suites to Transport Layer Security (TLS)" (https://tools.ietf.org/html/rfc6209), "RFC 6367: Addition of the Camellia Cipher Suites to Transport Layer Security (TLS)" (https://tools.ietf.org/html/rfc6367).

Regarding public key cryptosystems, the DSA algorithm that relies on the complexity of the discrete logarithm problem for security was deprecated. DSA is not vulnerable at this point in time, but there has been a shift to use of ECDSA, which reduces cryptographic processing using elliptic curve operations (ECDSA is not the only solution for signatures, as the cipher suites that use RSA for encryption and digital signatures remain). Meanwhile, DH used for key exchange is still not deprecated, along with ECDH. When using DH and ECDH, only the DHE and ECDHE varieties that generate keys that change each time (ephemeral keys) to fulfill forward secrecy*[58] are included on the cipher suites list. Regarding elliptic curve cryptography, based on discussion of pervasive monitoring*[59] at the IETF in recent years, it is recommended that in addition to Curve*[60] algorithms such as secp256r1 (Curve P-256) developed by NIST, the Curve25519*[61] algorithm presented by D.J. Bernstein at PKC2006 should also be implemented. The debate surrounding Curve is expected to come up again as a hot topic at IETF-94 held in Yokohama, and SSR2015 (The 2nd International Conference on Research in Security Standardisation) held in Japan in December of this year*[62].

(2) Simplification of the message flow and encryption of the Handshake message.

Up until TLS 1.2, the Handshake involved clients sending a cipher suites list to the server, and the server selecting one of the methods sent. On the other hand, in TLS 1.3 this laborious behavior has been eliminated, and the client now begins by sending one cipher suite without offering a choice. This reduces the key sharing for encryption and guaranteeing the integrity of data from a four way process to a three way one, as shown in Figure 16. Furthermore, in TLS 1.2 and earlier the encryption took place from the Finished message, but in TLS 1.3 this has been changed so keys are prepared in advance, and part of the Handshake message is also encrypted before the Master Secret is shared.

(3) Reorganization of pseudo-random number generation functions, and changes to the Master Secret calculation method and key derivation processes.

When encrypting Handshake messages, key sharing is carried out using a key derivation function that employs HMAC, which is specified in RFC 5869. Along with this change, the derivation method for the Master Secret has also been significantly revised, with separate encryption keys used in each phase. At this time, we expect that keys known as the Static Secret and Ephemeral Secret will be generated in advance along with the Master Secret, and used in steps to encrypt the Handshake message. The Master Secret is also designed to be generated from these two advance keys. Furthermore, although the actual keys used for symmetric key cryptography are derived from these three pieces of key data, because AEAD carries out encryption and MAC (message authentication code) assignment at the same time, the MAC key generation process has been eliminated.

*58 IIJ IIR Vol.22 "1.4.2 Forward Secrecy" (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol22_EN.pdf).

*59 "RFC 7258: Pervasive Monitoring Is an Attack" (https://tools.ietf.org/html/rfc7258).

*60 National Institute of Standards and Technology, "FIPS PUB 186-4, Digital Signature Standard (DSS)" (http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf).

*61 "A state-of-the-art Diffie-Hellman function" (http://cr.yp.to/ecdh.html).

*62 At SSR2015 (http://ssr2015.com/), which is to be held in Tokyo in December, it is expected that the topic of cryptographic algorithm selection including Curves will be discussed. The subject of revisions to RFC4492 (https://tools.ietf.org/html/rfc4492), which regulates cipher suites related to elliptic curves, was discussed at IETF-94 (https://www.ietf.org/proceedings/94/slides/slides-94-tls-0.pdf). The upgrade of the RSA signature format was also touched upon at the same conference. More specifically, the topic was the upgrade of RSASSA-PKCS1-v1_5 (defined in PKCS#1 version 1.5) to RSASSA-PSS (https://tools.ietf.org/html/rfc3447) (https://www.ietf.org/proceedings/94/slides/slides-94-tls-4.pdf).

This demonstrates that a variety of approaches are being evaluated, and transparent discussions about whether TLS 1.3 is really a secure protocol are still underway. Another direction being explored is the attempts to verify whether a given protocol is secure using formal verification tools such as ProVerif[*63]. In the same way that descriptions of provable security are required when a new cryptographic algorithm is proposed, we may come to similar common understanding for secure protocols as well.

■ Eliminating Factors that Trigger Implementation Issues

When it comes to using cryptographic algorithms or pseudo-random number generator modules, there are issues with the actual implementers not being aware of things the designer considers obvious. Some examples of this are issues with the reuse of public keys when the private key has been shared unintentionally, and implementations in which the data encryption key is hard coded, and the same key used for encryption every time[*64]. In addition to discrepancies occurring upon implementation, the lack of consensus is considered to be a primary factor that triggers vulnerabilities. Another issue is the fact that specifications such as RFC are written in natural language, so there is a certain degree of ambiguity to them, and some implementers may interpret them differently. We will need to evaluate the documentation and composition of the TLS 1.3 draft with this in mind. Consequently, in addition to removing unnecessary parts of the protocols themselves, we believe that any ambiguity in the descriptions within should also be removed.

1.5 Conclusion

This report has provided a summary of security incidents to which IIJ has responded. In this report, we examined route hijacking and the latest status of TLS 1.3. 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)
Yoshinobu Matsuzaki, Technology Planning Office, Network Division, IIJ (1.4.1 Route Hijacking)
Yuji Suga (1.4.2 The Latest Status of TLS 1.3)
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

[*63] Arai, Watanabe, Sakurada, Formal Verification of the TLS 1.3 Handshake Protocol Using ProVerif, 3C2-1, Computer Security Symposium 2015 (http://www.iwsec.org/css/2015/program.htm#i3C2) (in Japanese). There have also been reports of attacks on TLS 1.3 using other verification tools (https://www.ietf.org/mail-archive/web/tls/current/msg18215.html)

[*64] See the following PKI Day 2012 presentation materials (http://www.jnsa.org/seminar/pki-day/2012/data/PM02_suga.pdf) (in Japanese) or CRYPTREC Symposium 2015 materials (http://cryptrec.go.jp/topics/cryptrec_20150424_symposium2015_presentation.html) (in Japanese) for more information. There is also a method that takes into account the misuse of random data (https://tools.ietf.org/html/rfc6979). For DSA and ECDSA, random data is required each time for signing. However, there are moves to reduce implementation errors by making this deterministic depending on the data subject to signature.