IIJ
Internet Initiative Japan

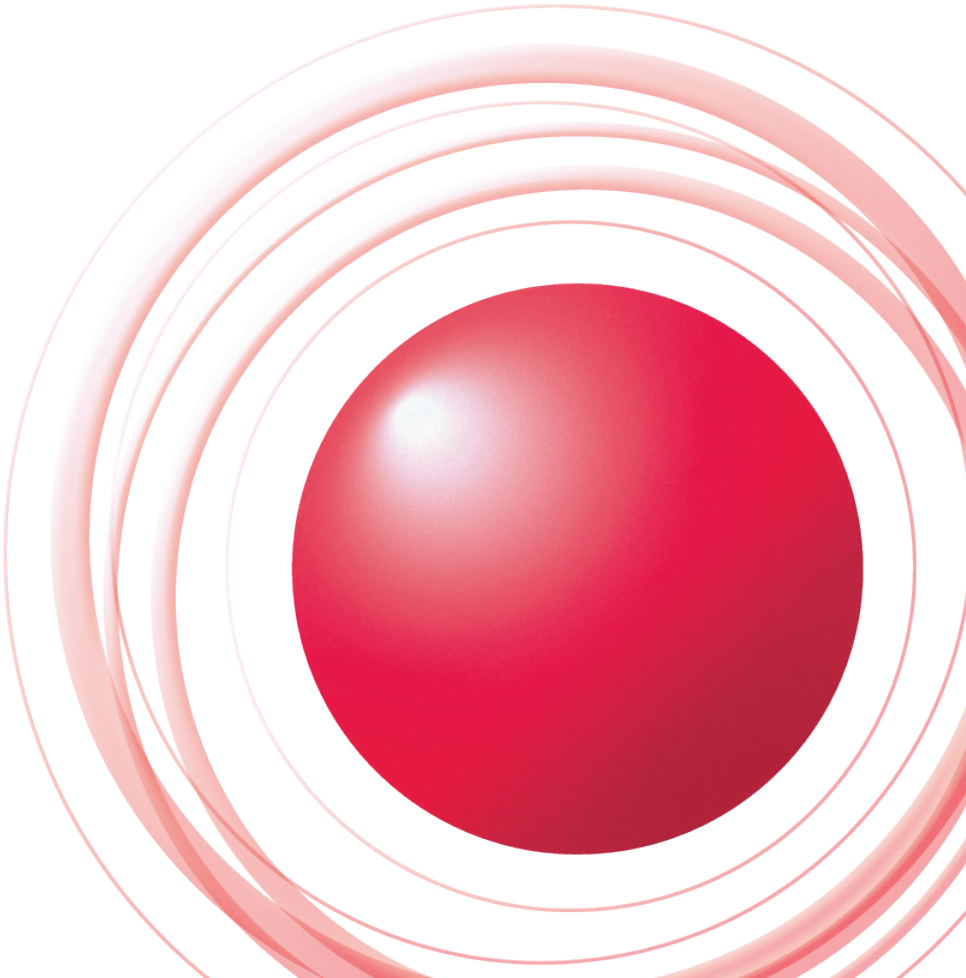
Internet Infrastructure Review Vol.24

August 2014

Infrastructure Security
OpenSSL Vulnerabilities

Broadband Traffic Report
Traffic Volumes Rise Steadily Over the Past Year, and HTTPS Use Expands

Technology Trends
The Environment Surrounding DNS



Internet Infrastructure Review

Vol.24 August 2014

■ To download current and past issues of the Internet Infrastructure Review in PDF format, please visit the IIJ website at http://www.iij.ad.jp/en/company/development/iir/.

Executive Summary

On April 8, 2014, a security advisory that outlined a vulnerability discovered in OpenSSL and called for measures to be taken was published, and a range of companies were forced to take urgent action. OpenSSL is open source software that implements a system called SSL, which is used when encrypting and transferring personal or confidential information, such as for online shopping or Internet banking. It is used extensively in Unix-like environments. The vulnerability that was discovered apparently allowed remote access to a relatively large slice of memory space on servers. If exploited, data such as passwords and private keys could be easily stolen, so it posed a serious threat. As a result it was given the name **Heartbleed**.

In July there was also a major leak of customer information at a prominent company in the field of education. This incident involved a contract employee who took the personal information of customers off premises and sold it to what are known as list traders. The company at which the leak occurred stated they have earmarked a total of 20 billion yen for compensation. This figure is apparently equal to the company's projected net profit for the current fiscal year. Companies have a heavy responsibility to manage the personal information of their customers, so the losses suffered in the event that an information leak does occur will have a considerable impact on their business.

This report discusses the results of the various ongoing surveys and analysis activities that IIJ carries out to support the Internet infrastructure and enable our customers to continue to use it safely and securely. We also regularly present summaries of technological development as well as important technical information.

In the "Infrastructure Security" section, we give a month-by-month chronological summary of major incidents observed during the three months from April 1 to June 30, 2014, and report on the results of our statistics gathering and analyses for the entire period. We also present our focused research for this period, including an explanation of the OpenSSL vulnerability disclosed on April 8, as well as analysis results and countermeasures for the "Vawtrak" malware that steals authentication information for Japanese financial institutions. Additionally, we discuss security checks and audit systems for cloud services.

In the "Broadband Traffic Report" section, we analyze changes in the average monthly traffic over IIJ's broadband access services for the past seven years since 2007, and report the conclusions we have drawn regarding long-term broadband traffic trends. We also analyze traffic data for the week of May 26 to June 1, 2014, and compare the results with those from the last survey spanning June 3 to June 9, 2013, followed by a report on our detailed analysis of changes in traffic trends over this past year.

In the "Technology Trends" section, we discuss the latest trends in the environment surrounding DNS, which an important Internet service. In particular, we cover the name collision issue that has emerged due to the addition of TLDs in recent years, and look at the current practice of DNS-based communication control that content providers and others are employing, as well as the issues involved. We also explain the current state of attacks on DNS in detail, along with their countermeasures.

Through activities such as these, IIJ continues to strive towards improving and developing our services on a daily basis while maintaining the stability of the Internet. We will keep providing a variety of solutions that our customers can take full advantage of as infrastructure for their corporate activities.

Author:

Toshiya Asaba
President and CEO, IIJ Innovation Institute Inc. President and CEO, Stratosphere Inc. Mr. Asaba joined IIJ in its inaugural year of 1992, becoming involved in backbone construction, route control, and interconnectivity with domestic and foreign ISPs. He was named IIJ director in 1999, and executive vice president in charge of technical development in 2004. When the IIJ Innovation Institute Inc. was founded in June 2008, Mr. Asaba became its president and CEO. When Stratosphere Inc. was founded in April 2012, he also became president and CEO of that organization.

OpenSSL Vulnerabilities

In this report, we discuss the discovery of a series of OpenSSL vulnerabilities that have had a significant impact, and examine the Vawtrak malware that steals authentication information for online banking, etc. We also take a look at auditing systems for cloud computing security.

1.1 Introduction

This report summarizes incidents to which IIJ responded, based on general information obtained by IIJ itself related to the stable operation of the Internet, information from observations of incidents, information acquired through our services, and information obtained from companies and organizations with which IIJ has cooperative relationships. This volume covers the period of time from April 1 through June 30, 2014. Continuing on from the last survey period, a number of hacktivism-based attacks were made by Anonymous and other groups. New OpenSSL vulnerabilities that allowed encrypted communications to be intercepted through MITM attacks were also discovered, and had a widespread effect. There were also incidents in which users of a number of Web services in Japan were infected with malware through altered content located on the servers of CDN providers. In June, there were large-scale DDoS attacks on an e-voting system in Hong Kong and also on online games. These examples show that many security-related incidents continue to occur on the Internet.

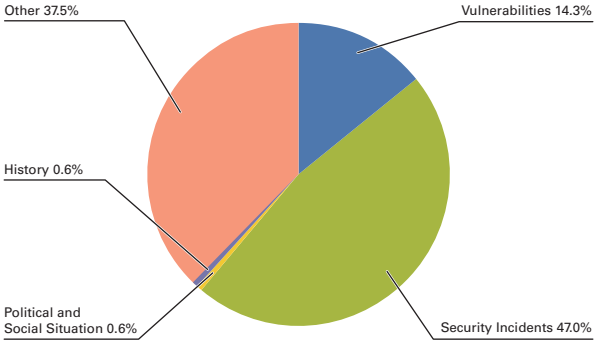


Figure 1: Incident Ratio by Category (April 1 to June 30, 2014)

1.2 Incident Summary

Here we discuss the IIJ handling and response to incidents that occurred between April 1 and June 30, 2014. 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. In April website defacements and information leaks affected a number of government-related websites in Israel (OpIsrael). Attacks were also made between India and Pakistan in the same month. In May, website defacements and DDoS attacks occurred in relation to territorial disputes between the Philippines and China. Attacks on the Chinese government and related agencies are still continuing (OpChina). Similarly, website defacements, information leaks, and DDoS attacks are occurring

*1 Incidents discussed in this report are categorized as vulnerabilities, political and social situation, history, security incidents and 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.

between China and Vietnam. In June there were attacks related to the FIFA World Cup soccer tournament held in Brazil. These targeted a number of websites, including Brazilian government agencies and TV stations. Attacks on companies sponsoring the World Cup were also planned, but in the end none were very large in scale. Other attacks by hacktivists such as Anonymous continued on government and government-related websites around the world. Unknown attackers claiming affiliation with the Syrian Electronic Army continued to hijack SNS accounts and deface websites, with affected accounts including those of media organizations such as The Wall Street Journal and Reuters.

■ Vulnerabilities and their Handling

During this period fixes were released for Microsoft products including Windows*2, Internet Explorer*3*4*5*6, and Office*7*8*9. Updates were also made to Adobe Systems' Adobe Flash Player, Adobe Reader, and Adobe Acrobat. A quarterly update was released for Oracle's Java SE, fixing many vulnerabilities. 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 caused named to terminate abnormally when receiving specially crafted DNS requests were also discovered and fixed.

Vulnerabilities in the OpenSSL cryptographic software library that could allow sensitive data such as private keys to leak, or that may facilitate MITM attacks*10, were also discovered and fixed. In particular, alerts were issued by a number of organizations including the IPA regarding the former vulnerability, known as Heartbleed. A number of attacks in which this flaw was actually exploited also occurred. See "1.4.1 OpenSSL Vulnerabilities" for more information. Several serious OpenSSL vulnerabilities have been discovered in the past, and when vulnerabilities are found in a widely used library like this, the impact is broad. As a result, a number of approaches are being taken to resolve issues, such as the establishment of the Core Infrastructure Initiative*11 for supporting key open source projects like OpenSSL, and the launch of the LibreSSL project that aims to develop a more secure implementation*12.

Another fix was also released for a vulnerability in the Apache Struts Web application framework that allowed ClassLoader to be manipulated, as a patch issued in March had been bypassed. After it was established that this vulnerability also affected Apache Struts 1, for which support had already ended in 2013, service was temporarily suspended on several websites to take measures such as the application of fixes. A number of attacks that actually exploited this vulnerability were also confirmed*13.

■ Unauthorized Login Through Identity Fraud

Since last year there have been many attempts to steal user IDs and passwords, and log in without authorization through identity fraud presumably using lists of these IDs and passwords. These activities continued in the current survey period. There were a large number of unauthorized login attempts, thought to use lists of IDs and passwords, on sites including

*2 "Microsoft Security Bulletin MS14-025 - Important: Vulnerability in Group Policy Preferences Could Allow Elevation of Privilege (2962486)" (https://technet.microsoft.com/library/security/ms14-025).
*3 "Microsoft Security Bulletin MS14-018 - Critical: Cumulative Security Update for Internet Explorer (2950467)" (https://technet.microsoft.com/library/security/ms14-018).
*4 "Microsoft Security Bulletin MS14-021 - Critical: Security Update for Internet Explorer (2965111)" (https://technet.microsoft.com/library/security/ms14-021).
*5 "Microsoft Security Bulletin MS14-029 - Critical: Security Update for Internet Explorer (2962482)" (https://technet.microsoft.com/library/security/ms14-029).
*6 "Microsoft Security Bulletin MS14-035 - Critical: Cumulative Security Update for Internet Explorer (2969262)" (https://technet.microsoft.com/library/security/ms14-035).
*7 "Microsoft Security Bulletin MS14-024 - Important: Vulnerability in a Microsoft Common Control Could Allow Security Feature Bypass (2961033)" (https://technet.microsoft.com/library/security/ms14-024).
*8 "Microsoft Security Bulletin MS14-017 - Critical: Vulnerabilities in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (2949660)" (https://technet.microsoft.com/library/security/ms14-017).
*9 "Microsoft Security Bulletin MS14-034 - Important: Vulnerability in Microsoft Word Could Allow Remote Code Execution (2969261)" (https://technet.microsoft.com/library/security/ms14-034).
*10 See the following article by the discoverer, Mr. Kikuchi of Lepidum Co. Ltd., for more details. "CCS Injection Vulnerability" (http://ccsinjection.lepidum.co.jp).
*11 See the following Linux Foundation blog post for more details. "Announcing Rapid Progress on Core Infrastructure Initiative" (http://www.linuxfoundation.org/news-media/blogs/browse/2014/06/announcing-rapid-progress-core-infrastructure-initiative).
*12 LibreSSL (http://www.libressl.org/).
*13 For example, see the following National Police Agency announcement. "Regarding the detection of communications targeting an Apache Struts 2 vulnerability" (http://www.npa.go.jp/cyberpolice/detect/pdf/20140427.pdf) (in Japanese).

April Incidents

1st: The JPCERT Coordination Center announced they would transition from displaying their own metrics for the severity of vulnerabilities on the JVN vulnerability countermeasure information portal site to using the Common Vulnerability Scoring System (CVSS).
"JVN adopts the Common Vulnerability Scoring System (CVSS) international standard for displaying vulnerability severity"
(https://www.jpcert.or.jp/pr/2014/PR20140401-jvn.pdf) (in Japanese).

2nd: The Ministry of Internal Affairs and Communications announced their "Information Security Guidelines for Cloud Services," which describes security measures that cloud service providers should implement, and templates for terms of agreement that should be established with users.
"Announcement of Information Security Guidelines for Cloud Service"
(http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/140402_01.html).

8th: A vulnerability (CVE-2014-0160) in OpenSSL that could allow data in memory to leak to a third party due to a flaw in the TLS Heartbeat extension processing was discovered and fixed.
See the following explanation for more details. "The Heartbleed Bug" (http://heartbleed.com/).

8th: Issues such as reboots or hang-ups were reported on routers with outdated firmware, caused by communications sent from unspecified hosts. For example, Yamaha Corporation issued the following announcement. "Regarding reboots and other issues on Yamaha routers caused by Internet-based attacks" (http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/attack-from-internet-201404.html) (in Japanese).

9th: Microsoft published their Security Bulletin Summary for April 2014, and released two critical updates including MS14-017 and MS14-018, as well as two important updates.
"Microsoft Security Bulletin Summary for April 2014" (https://technet.microsoft.com/library/security/ms14-apr).

9th: Microsoft ended support for Windows XP, Microsoft Office 2003, and Internet Explorer 6.
"Windows XP support has ended" (http://windows.microsoft.com/en-us/windows/end-support-help).

13th: Google improved the Verify Apps feature in Android to offer a function that constantly monitors whether there are security issues in installed apps.
See the following Google Android Official Blog post for more details. "Expanding Google's security services for Android"
(http://officialandroid.blogspot.com/2014/04/expanding-googles-security-services-for.html).

14th: A vulnerability in the Android version of Adobe Reader Mobile that could allow remote arbitrary code execution was discovered and fixed.
"APSB14-12: Security update available for Adobe Reader Mobile" (http://helpx.adobe.com/security/products/reader-mobile/apsb14-12.html).

15th: JPRS issued an alert due to an increase in cache poisoning attacks targeting cache DNS servers without source port randomization enabled.
"(Critical) Regarding the double checking of DNS server configurations in light of the increasing danger of cache poisoning attacks"
(http://jprs.jp/tech/security/2014-04-15-portrandomization.html) (in Japanese).

15th: Oracle released their quarterly scheduled update for a number of products including Oracle, fixing a total of 104 vulnerabilities, including 37 in Java SE.
"Oracle Critical Patch Update Advisory - April 2014" (http://www.oracle.com/technetwork/topics/security/cpuapr2014-1972952.html).

15th: It was announced an attack that exploited an OpenSSL vulnerability (CVE-2014-0160) had been made on the website of the Canada Revenue Agency, and the social security numbers of around 900 taxpayers had leaked. On April 17 a student was arrested on suspicion of carrying out the attack.
See the following official announcement by the Canada Revenue Agency for more details. "Notice - Heartbleed bug vulnerability"
(http://www.cra-arc.gc.ca/gncy/sttmnt2-eng.html).

16th: The National Institute of Infectious Diseases announced that email account user names and passwords had been stolen through emails impersonating a webmail administrator, resulting in spam being sent.
"Regarding the unauthorized use of National Institute of Infectious Diseases email accounts, and the sending of spam"
(http://www.nih.go.jp/niid/ja/maintenance/4575-incidence140416.html) (in Japanese).

22nd: The U.S. National Institute of Standards and Technology (NIST) presented a draft of SP 800-90/90A that omitted the Dual_EC_DRBG pseudorandom number generator algorithm for which security concerns had been raised.
"NIST Removes Cryptography Algorithm from Random Number Generator Recommendations" (http://www.nist.gov/itl/csd/sp800-90-042114.cfm).

24th: A fix for an Apache Struts 2 vulnerability (CVE-2014-0094) was deemed inadequate, and vulnerabilities (CVE-2014-0112) (CVE-2014-0113) that allowed specific manipulations by third parties were discovered and fixed.
Alerts were issued regarding CVE-2014-0094, for example by the IPA on April 17, and subsequently alerts were updated to include these vulnerabilities. See "Security Alert for Vulnerabilities in Apache Struts 2 (CVE-2014-0094) (CVE-2014-0112) (CVE-2014-0113)"
(http://www.ipa.go.jp/security/ciadr/vul/20140417-struts.html) (in Japanese) for more details.

28th: Microsoft announced there was a vulnerability with no fix available that could allow remote code execution in a number of versions of Internet Explorer.
"Microsoft Security Advisory (2963983) Vulnerability in Internet Explorer Could Allow Remote Code Execution"
(https://technet.microsoft.com/library/security/2963983).

29th: A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"Security updates available for Adobe Flash Player" (http://helpx.adobe.com/security/products/flash-player/apsb14-13.html).

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

*Dates are in Japan Standard Time

mobile phone user support sites, e-commerce sites, game sites, and SNS. In a number of these incidents tangible damage was caused, such as the exchange of site points for gift points on other sites without authorization. Other incidents in which messaging app accounts were used without authorization involved techniques such as the sending of messages impersonating hijacked account owners to friends suggesting they purchase digital currency. This demonstrates that unauthorized access attempts thought to use lists of IDs and passwords are ongoing, so continued care must be taken to review the management of IDs and passwords you use, and stay abreast of the latest techniques.

■ An Increase in Web Alterations and Attacks Targeting Legitimate Software

During this survey period, there were many incidents in which websites were altered to redirect visitors to malicious software. A CDN service server was compromised in May, resulting in the alteration of a number of corporate sites. In addition to redirecting visitors to other sites to install malicious software, it was revealed these incidents also involved the alteration of legitimate content such as update files placed on the servers by companies using the service, in an attempt to get users to install files containing malware. Similar cases include reports of malware infections through altering the distribution point of legitimate software for industrial control systems*14. In June there were also incidents of redirection from an advertising provider to a malicious website masquerading as an Adobe Flash Player download site that prompted the download of a malicious program*15. This happened when the advertising provider in question received specific malicious advertisements mixed in with those received from another advertising provider in the U.S. for distribution in Japan. We believe this kind of malware activity that exploits trust in legitimate software will continue in the future.

■ Bitcoin

As the Bitcoin virtual currency becomes used in more and more transactions, a variety of incidents have occurred. During the current survey period, the Mt. Gox Bitcoin exchange that went bankrupt in February was issued with a provisional administration order by the Tokyo District Court after it abandoned its filing for rebuilding under the Civil Rehabilitation Act. Also, partly as a result of these events, the Consumer Affairs Agency issued an alert regarding the trading and use of Internet-based virtual currencies such as Bitcoin*16. In the United States, the U.S. Securities and Exchange Commission issued an alert regarding theft and investment fraud in relation to virtual currencies including Bitcoin*17. Meanwhile, there was lively debate around the world regarding Bitcoin transactions, such as the Federal Election Commission of the United States voting to allow Bitcoin donations during elections. A string of attacks on virtual currency exchanges and account management services also continued, including many DDoS attacks on their websites, and thefts of virtual currency through server compromises.

■ DDoS Attacks

A number of large-scale DDoS attacks occurred during this period. In May a DDoS attack was made on UltraDNS*18. The attack is said to have had a magnitude of 100 Gbps, and it affected the services of a number of companies including Salesforce. In June services such as Evernote and Feedly were also targeted in DDoS, and in some cases demands for money were made*19. In Hong Kong, a large-scale DDoS attack that reached a peak of 300 Gbps was made on the voting system site of an organization pushing for democratization. In May there was also a sharp increase in DNS queries at multiple ISPs in Japan, causing outages at a number of ISPs. In June there were large-scale DDoS attacks targeting the Web servers and game servers for an online game, causing service to be suspended for several days among other damages*20.

*14 For example, the following F-Secure blog post explains the Havex malware that targets ICS/SCADA systems. It demonstrates that one infection technique involves compromising an ICS vendor site and using a software installer containing a Trojan. “Havex Hunts For ICS/SCADA Systems” (http://www.f-secure.com/weblog/archives/00002718.html).

*15 Symantec Security Response blog “Nico Nico Users Redirected to Fake Flash Player” (http://www.symantec.com/connect/blogs/nico-nico-users-redirected-fake-flash-player).

*16 Consumer Affairs Agency, “Regarding the use of Internet-based virtual currency such as Bitcoin” (http://www.caa.go.jp/adjustments/pdf/140428adjustments_1.pdf) (in Japanese).

*17 U.S. Securities and Exchange Commission, “Investor Alert: Bitcoin and Other Virtual Currency-Related Investments” (http://investor.gov/news-alerts/investor-alerts/investor-alert-bitcoin-other-virtual-currency-related-investments#.U4RTq_l_v24).

*18 See the following InfoSec Handlers Diary Blog post for more details about this incident. “UltraDNS DDOS” (https://isc.sans.edu/diary/UltraDNS+DDOS/18051).

*19 See the following post on the blog of Feedly, one of the companies affected, for more details. “Denial of service attack [Neutralized]” (http://blog.feedly.com/2014/06/11/denial-of-service-attack/).

*20 For example, see the following announcement (http://pso2.jp/players/news/?id=3835) (in Japanese).

May Incidents

2nd: Microsoft released an update for a vulnerability published several days before that could allow remote code execution in a number of versions of Internet Explorer.
"Microsoft Security Bulletin MS14-021 - Critical: Security Update for Internet Explorer (2965111)"
(https://technet.microsoft.com/library/security/ms14-021).

8th: The U.S. Securities and Exchange Commission issued an alert regarding investment in virtual currencies such as Bitcoin due to the risk of being caught up in crimes such as investment fraud.
"Investor Alert: Bitcoin and Other Virtual Currency-Related Investments"
(http://investor.gov/news-alerts/investor-alerts/investor-alert-bitcoin-other-virtual-currency-related-investments).

9th: A vulnerability in BIND 9.10.0 that could allow DoS attacks from external sources due to implementation issues was discovered and fixed.
"Critical: BIND 9.10.0 vulnerability (DNS service outage) (disclosed May 9, 2014)
(http://jprs.jp/tech/security/2014-05-09-bind9-vuln-prefetch.html) (in Japanese).

9th: The Federal Trade Commission (FTC) of the United States issued a complaint regarding the Snapchat photo sharing app, which provides a service that can be configured to remove photo data from other parties' devices. It alleged that false claims had been made because this data did not actually disappear, and pointed out problems with their management of personal information regarding the leak of 4.6 million pieces of personal information in January.
"Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False"
(http://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were).

14th: Microsoft published their Security Bulletin Summary for May 2014, and released two critical updates including MS14-022 and MS14-029, as well as six important updates.
"Microsoft Security Bulletin Summary for May 2014" (https://technet.microsoft.com/library/security/ms14-may).

14th: A number of vulnerabilities in Adobe Reader and Acrobat that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB14-15: Security Updates available for Adobe Reader and Acrobat" (http://helpx.adobe.com/security/products/reader/apsb14-15.html).

14th: A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB14-14: Security updates available for Adobe Flash Player" (http://helpx.adobe.com/security/products/flash-player/apsb14-14.html).

14th: The Bill on Cyber Security was passed by the Lower House of Japan's Diet. It was subsequently referred to the Upper House, but on June 20 it was marked for further examination.
Upper House, "Bill on Cyber Security" (http://www.sangiin.go.jp/japanese/joho1/kousei/gian/186/meisai/m18605186035.htm) (in Japanese).

15th: The JPCERT Coordination Center issued an alert due to many confirmed incidents of attacks using known vulnerabilities in Movable Type to place malicious files on sites or embed iframes or obfuscated JavaScript that redirects to attack sites.
"JPCERT/CC Alert 2014-05-15 Alert regarding the usage of old versions of Movable Type" (https://www.jpcert.or.jp/english/at/2014/at140024.html).

19th: A suspect arrested and charged with crimes such as the forcible obstruction of business in relation to a series of incidents linked to the Remote Control Virus had his bail revoked after it was found he had sent emails during the trial that identified the author as the perpetrator. The suspect later confessed he was behind the incidents, admitting responsibility for the crime.

20th: The FBI announced they had arrested over 100 people, including the suspected co-creators of the Blackshades RAT that steals files and account information.
See the following FBI announcement for more information about this incident. "Manhattan U.S. Attorney And FBI Assistant Director-In-Charge Announce Charges In Connection With Blackshades Malicious Software That Enabled Users Around The World To Secretly And Remotely Control Victims' Computers" (http://www.justice.gov/usao/nys/pressreleases/May14/BlackshadesPR.php).

20th: The Ministry of Economy, Trade and Industry amended the Standards for Handling Software Vulnerability Information and Others, including the addition of criteria for disclosing vulnerabilities when the product developer cannot be contacted.
"Regarding amendments to the Standards for Handling Software Vulnerability Information and Others"
(http://www.meti.go.jp/policy/netsecurity/default.htm) (in Japanese).

20th: The IPA announced it would put together a team for preparing a Cyber Rescue Squad (provisional) to support organizations affected by targeted attacks by limiting damages, deterring and reducing reoccurrence, and implementing swift countermeasures.
"Press Release: Team for preparing a 'Cyber Rescue Squad' established on May 20" (https://www.ipa.go.jp/about/press/20140520.html) (in Japanese).

22nd: A vulnerability in Microsoft's Internet Explorer 8 with no fix available that could allow arbitrary code execution was discovered and disclosed.
This vulnerability was fixed on June 11 in "Microsoft Security Bulletin MS14-035 - Critical: Cumulative Security Update for Internet Explorer (2969262)" (https://technet.microsoft.com/library/security/ms14-035).

22nd: The "USA Freedom Act" NSA surveillance reform bill passed in the U.S. House of Representatives.
Librarian of Congress, "Bill Summary & Status 113th Congress (2013 - 2014) H.R.3361 All Information"
(http://thomas.loc.gov/cgi-bin/bdquery/z?d113:HR03361:@@@L&summ2=m&).

27th: An incident occurred in which Apple devices such as iPhones were remotely locked and demands for money made in a number of countries including Australia.
It is believed that the Find My iPhone feature that Apple provides was exploited in these incidents, but details of the technique used have not been revealed.

29th: Outages occurred at a number of providers due to a sudden increase in queries to their DNS servers.

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

*Dates are in Japan Standard Time

■ Government Agency Initiatives

Government agency security countermeasure activities included the Ministry of Internal Affairs and Communications announcing their "Information Security Guidelines for Cloud Services" in April. The previous "Guidelines for Information Security Measures for ASP/SaaS"*21 put together in 2008 stipulated information security measures that cloud providers should implement. Recommendations for cloud providers regarding agreements with users and practices between providers have now also been incorporated. This was done due to the spread of usage covering multiple cloud services and providers, such as coordination between infrastructure-based cloud services such as PaaS and IaaS, and cloud services that provide applications such as ASP and SaaS.

In June, the Amended Act Prohibiting Child Prostitution and Pornography was passed. These revisions banned the mere possession of photos or video of child pornography by individuals, and established new stipulations for the efforts of ISPs regarding Internet usage.

Also in June, the Bill on Cyber Security that aims to improve the government response to cyber attacks passed the Lower House. This included initiatives focused on furnishing Japan and local governments with the ability to deal with cyber attacks. Some examples are the establishment of a "Cyber Security Strategic Headquarters" headed by the Chief Cabinet Secretary, and improvements to government response capability and functionality, such as enabling recommendations to be made to government agencies regarding countermeasures to implement. The bill also promoted initiatives that improve response capability for cyber attacks through public-private collaboration, such as having private sector critical infrastructure providers provide assistance with countermeasures. This bill was later deliberated in the Upper House, but was not passed in the current Diet session, so it has been carried over to the next session.

Discussion of legal measures for resolving issues with promoting the use and application of personal data also took place at the "Investigative Commission on Personal Data." A "Policy Outline of the Institutional Revision for Utilization of Personal Data" was announced, covering the introduction of a framework for allowing information to be provided to third parties without a user's consent under certain conditions. The outline also detailed a fundamental system framework and the utilization of voluntary private sector initiatives to supplement this, as well as effective ways of enforcing the system through the development of an independent third-party authority.

The Ministry of Economy, Trade and Industry announced amendments to the "Standards for Handling Software Vulnerability Information and Others." It was decided that when no agreement on disclosure can be made with the product developer, such as when they cannot be contacted for an extended period of time, a decision on whether or not the vulnerability information should be disclosed will be made based on the opinion of an independent panel of experts.

■ **Attacks Targeting Online Banking**

During the current survey period attacks that used phishing or malware to target online banking information attracted attention. In April there were incidents of unauthorized login believed to involve the use of lists at a regional bank. Additionally, phishing sites and phishing emails targeting a number of financial institutions have been uncovered*22. Malware that targets Japanese financial institutions was also identified*23, demonstrating that increasingly sophisticated methods are being used. See "1.4.2 The Vawtrak Malware That Steals Authentication Information for Japanese Financial Institutions" for more information about malware-based attacks. In April, it was reported that account information including around 13,000 Internet banking IDs and passwords had been illegally stored on a server in Japan. It is thought that the information uncovered in this incident was stolen through virus infections that display fraudulent sites when an Internet banking site is used. This demonstrates that attacks targeting details such as the credit card and online banking authentication information of users in Japan for monetary gain continue, and because the methods used are becoming more and more refined, ongoing vigilance is required.

*21 Ministry of Internal Affairs and Communications "Guidelines for Information Security Measures for ASP/SaaS" (http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/asp_saas/) (in Japanese).

*22 See the Council of Anti-Phishing Japan site (http://www.antiphishing.jp/) (in Japanese) for alerts on various phishing campaigns.

*23 For example, see the following Trend Micro blog post "Increasing reports of the detection of the 'VAWTRAK' online banking fraud tool that targets credit card information in Japan" (http://blog.trendmicro.co.jp/archives/9192) (in Japanese).

June Incidents

S **3rd:** It was established that incidents of unauthorized access and the alteration of content and files affecting a number of sites from late May were due to the compromise of the CDN service provider they had been using.

S **3rd:** The United States Department of Justice announced a takedown to disrupt the GameOver Zeus malware that steals online banking information in a joint operation involving law enforcement agencies in over 10 countries. Related sites were seized and the alleged administrator was arrested.
Department of Justice, "U.S. Leads Multi-National Action Against 'Gameover Zeus' Botnet and 'Cryptolocker' Ransomware, Charges Botnet Administrator" (http://www.justice.gov/opa/pr/2014/June/14-crm-584.html). The National Police Agency provided assistance in Japan. See "International Botnet Takedown Operation" (http://www.npa.go.jp/cyber/goz/index.html) (in Japanese) for a description of this operation.

V **6th:** A vulnerability (CVE-2014-0224) in OpenSSL that could allow man-in-the-middle (MITM) attacks was discovered and fixed.
"OpenSSL Security Advisory [05 Jun 2014] SSL/TLS MITM vulnerability (CVE-2014-0224)" (https://www.openssl.org/news/secadv_20140605.txt).

V **11th:** Microsoft published their Security Bulletin Summary for June 2014, and released two critical updates including MS14-035 and MS14-036, as well as five important updates.
"Microsoft Security Bulletin Summary for June 2014" (https://technet.microsoft.com/library/security/ms14-jun).

V **11th:** 11th: A number of vulnerabilities in Adobe Flash Player that could allow arbitrary code execution were discovered and fixed.
"APSB14-16: Security updates available for Adobe Flash Player" (http://helpx.adobe.com/security/products/flash-player/apsb14-16.html).

V **12th:** A vulnerability (CVE-2014-3859) in BIND 9.10.x that could allow denial-of-service (DoS) attacks from outside was discovered and fixed.
Internet Systems Consortium, "CVE-2014-3859: BIND named can crash due to a defect in EDNS printing processing" (https://kb.isc.org/article/AA-01166/).

S **12th:** An alert was issued because approximately 80% of blog sites that use a Japan-oriented blog creation tool for which support had ended were being operated in a problematic configuration, causing them to be targeted by attackers.
See the following Kaspersky Lab blog post for more information. "Japanese blog creation tools targeted by attackers!" (http://blog.kaspersky.co.jp/obsolete-japanese-cms-targeted-by-criminals/) (in Japanese).

S **13th:** A large-scale DDoS attack was made on the e-voting system of an organization working towards the democratization of Hong Kong.
See the following blog post of Harvard University Internet Monitor Berkman Center for Internet & Society for more details. "DDoS Attacks in Hong Kong Target Pro-Democracy Websites" (https://blogs.law.harvard.edu/internetmonitor/2014/06/20/ddos-attacks-in-hong-kong-attack-silence-pro-democracy-websites/).

O **18th:** The Amended Act Prohibiting Child Prostitution and Pornography was passed, adding items prohibiting mere possession.
The revised act came into effect on July 15. See the following Ministry of Justice explanation for more details. "The bill for amending part of the Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children" (http://www.moj.go.jp/keiji1/keiji11_00008.html) (in Japanese).

S **19th:** An incident occurred in which an advertisement distribution server displayed advertisements that redirected visitors to a malicious site that presented itself as a notice prompting the update of Adobe Flash Player.
"<<Follow-up to press release regarding advertisement distribution issue>>" (http://www.microad.co.jp/news/detail.php?News_ID=252) (in Japanese).

O **19th:** The 12th Investigative Commission on Personal Data was held, and a "Policy Outline of the Institutional Revision for Utilization of Personal Data (commission proposal)" was laid out.
Office of the Prime Minister, "12th Investigative Commission on Personal Data - Agenda" (http://www.kantei.go.jp/jp/singi/it2/pd/dai12/gijisidai.html) (in Japanese).

O **27th:** The U.S. government published their 2013 Transparency Report.
See the following report for more details (http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013).

O **29th:** A published research paper revealed that Facebook had carried out psychological experiments involving the manipulation of the news feeds of approximately 700,000 users. It raised ethical concerns, attracting a lot of interest.
See the paper in question, "Experimental evidence of massive-scale emotional contagion through social networks" (http://www.pnas.org/content/111/24/8788.full).

S **30th:** Microsoft announced it had initiated a takedown of the 23 domains of the NO-IP dynamic DNS service, which had been used by the Bladabindi (NJrat) and Jenxcus (NJw0rm) malware families.
The Official Microsoft Blog, "Microsoft takes on global cybercrime epidemic in tenth malware disruption" (http://blogs.microsoft.com/blog/2014/06/30/microsoft-takes-on-global-cybercrime-epidemic-in-tenth-malware-disruption/). A statement was also issued by Vitalwerks Internet Solutions, LLC, which operates NO-IP. "No-IP's Formal Statement on Microsoft Takedown (https://www.noip.com/blog/2014/06/30/ips-formal-statement-microsoft-takedown/).

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

*Dates are in Japan Standard Time

Other

In April, JPRS issued an alert regarding the Kaminsky-type attack method*24, which was thought to have been behind an increase in cache DNS server access*25. Additionally, many new gTLD are currently being approved. As a result, JPNIC issued an alert regarding information leaks and service outages that may occur when the domain names used in internal networks, such as those as companies, collide with newly added domain names*26.

In April, South Korea's Financial Supervisory Service announced that the credit card information of about 200,000 users of multiple credit card companies had leaked. This came to light through an investigation into a server compromise at a POS terminal management company that occurred in December 2013. Other incidents involving business systems such as POS terminals include an information leak that occurred at a major U.S. retailer in November of last year. The incident in the United States involved the use of malware that targeted POS terminals, so US-CERT issued an alert in January*27. As a result of this incident, the Retail Cyber Intelligence Sharing Center (R-CISC) was established in May, serving as a retail-oriented organization for sharing and analyzing security information*28. There have also been reports of POS malware infections in Japan, so care will need to be taken with business systems such as these in the future.

In May, the suspect arrested and charged with the forcible obstruction of business in relation to a series of incidents involving the Remote Control Virus, which garnered a lot of attention the year before last, had his bail revoked after he was linked to emails from someone claiming to be the true culprit that were sent during the trial. He later confessed he was behind the crimes.

In May there were a number of incidents in regions such as Australia in which Apple devices such as iPhones and iPads were locked and ransom demands made. It is believed this involved an unknown entity illegally using accounts for a management service used when a device is lost.

Also in May, the Court of Justice of the European Union ruled that Google Spain and Google Inc. were responsible for deleting links to sites containing personal information in search results when requested by users*29. Regarding the handling of data containing personal information, with the requirement for administrators of personal information to delete said data when requested by the relevant individuals (the so-called "Right to be Forgotten") currently under debate in Europe as part of the EU General Data Protection Regulation*30, we believe a range of initiatives aimed at improving the protection of personal information will continue to emerge.

*24 See "1.4.1 DNS Cache Poisoning" in IIR Vol.2 (http://www.iij.ad.jp/development/iir/pdf/iir_vol02.pdf) (in Japanese) for more information.

*25 Japan Registry Services, "(Critical) Regarding the double checking of DNS server configurations in light of the increasing danger of cache poisoning attacks" (http://jprs.jp/tech/security/2014-04-15-portrandomization.html) (in Japanese).

*26 Japan Network Information Center (JPNIC), "Name collision issues resulting from the adoption of large numbers of new gTLD, and their countermeasures" (https://www.nic.ad.jp/ja/dom/new-gtld/name-collision/name-collision-report.pdf) (in Japanese).

*27 US-CERT, "Alert (TA14-002A) Malware Targeting Point of Sale Systems" (http://www.us- cert.gov/ncas/alerts/TA14-002A).

*28 Retail Cyber Intelligence Sharing Center (R-CISC), "Retailers Launch Comprehensive Cyber Intelligence Sharing Center" (http://www.rila.org/rcisc/home/Pages/default.aspx).

*29 Court of Justice of the European Union, "An internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties" (http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf).

*30 For more information about the EU General Data Protection Regulation (proposed) that is currently being worked on, see the following Japan Electronics and Information Technology Industries Association "Survey and analysis report regarding revision of EU data protection directives" (http://home.jeita.or.jp/page_file/20120427161714_IjwGedIUnB.pdf) (in Japanese).

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 Defense Service between April 1 and June 30, 2014.

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

There are many methods that can be used to carry out a DDoS attack, and the capacity of the environment attacked (bandwidth and server performance) will largely determine the degree of impact. Figure 2 categorizes DDoS attacks into three types: attacks on bandwidth capacity*31, attacks on servers*32, 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 388 DDoS attacks. This averages to 4.3 attacks per day, indicating a decrease in the average daily number of attacks compared to our prior report. Server attacks accounted for 78.6% of all incidents, while compound attacks accounted for 16.2%, and bandwidth capacity attacks 5.2%.

The largest attack observed during the period under study was classified as a compound attack, and resulted in 72.9 Mbps of bandwidth using up to 9,000 pps packets. Of all attacks, 94.8% ended within 30 minutes of commencement, 5.2% lasted between 30 minutes and 24 hours, and none lasted over 24 hours. The longest sustained attack was a server attack that lasted for 15 hours and 57 minutes. This shows there was a dramatic decrease in the number and bandwidth of attacks compared to the previous survey period. However, sporadic incidents of DrDoS attacks exploiting DNS and NTP are currently in the international spotlight, so continued vigilance is necessary.

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*33 and botnet*34 usage as the method for conducting DDoS attacks.

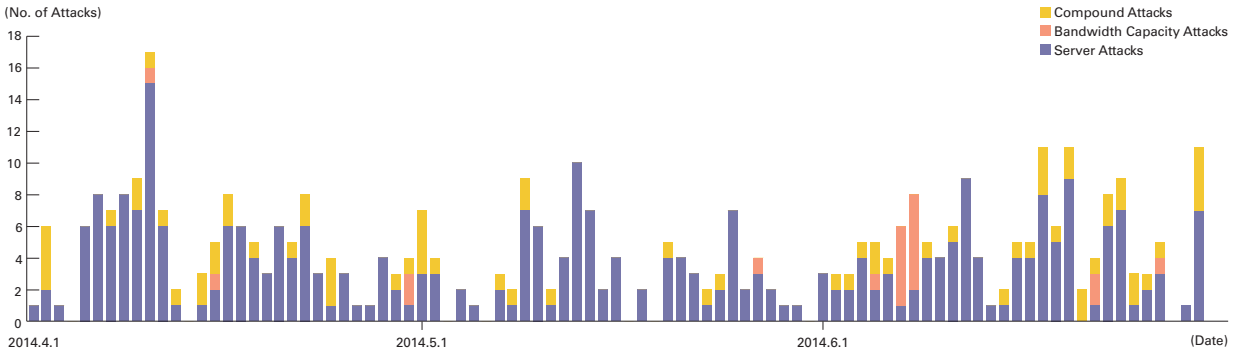


Figure 2: Trends in DDoS Attacks

*31 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.

*32 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.

*33 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.

*34 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.

■ Backscatter Observations

Next we present our observations of DDoS attack backscatter using the honeypots*35 set up by the MITF, a malware activity observation project operated by IIJ*36. By monitoring backscatter it is possible to detect some of the DDoS attacks occurring on external networks as a third party without any interposition.

For the backscatter observed between April 1 and June 30, 2014, 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 80/TCP port used for Web services, accounting for 22.6% of the total during the target period. Attacks were also observed on 53/UDP and 53/TCP used for DNS, and 22/TCP used for SSH, as well as 3477/TCP and 5000/TCP, which are normally not used. The DNS (53/UDP) backscatter observed in the last report continued, fluctuating while hovering at a daily average of around 1,500 packets. Care must be taken with regard to DDoS attacks and DNS cache poisoning attacks in the future.

Looking at the origin of backscatter thought to indicate IP addresses targeted by DDoS by country in Figure 3, the United States accounted for the largest ratio at 17.3%. Canada and China followed at 9.0% and 8.3%, respectively.

Looking at particularly large numbers of backscatter packets observed by port, there were attacks on Web servers (80/TCP) targeting a hosting provider in the U.S. that mainly provided services to Japan on April 15, and a hosting provider in Russia on April 16. Attacks on the servers of a CDN provider in the U.S. were also observed on June 30. Between April 6 and April 8 attacks on 3477/TCP were observed, but the attack target was not identified because the source IP address of the backscatter was a private address. On April 23 there were DNS (53/TCP) attacks on a Canadian hosting provider, and attacks on the same provider targeting 5000/TCP, 5001/TCP, and 6005/TCP occurred on June 21. Attacks on SSH (22/TCP) were also observed on June 23. On May 15 attacks on a range of TCP ports targeting a specific server in Russia were observed.

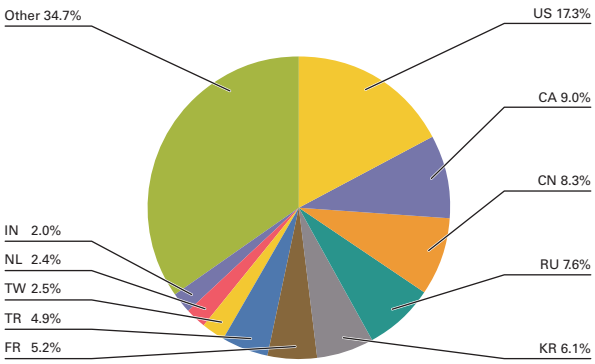


Figure 3: DDoS Attack Targets by Country According to Backscatter Observations

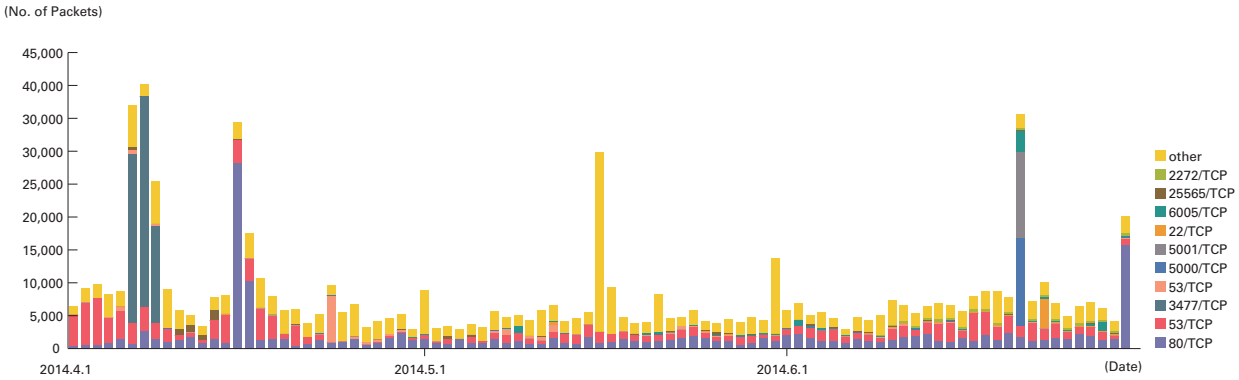


Figure 4: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)

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

*36 The mechanism and limitations of this observation method, as well as some of the results of IIJ's observations, are presented in IIR Vol.8 (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."

Notable DDoS attacks during the current survey period that were detected via IIJ's observations of backscatter included DDoS attacks on an online testing site in the U.S. state of Kansas that were reported by a number of news sites in early April. These attacks continued to be observed intermittently after they were reported. Other attacks were also detected on UltraDNS in the U.S. on May 1, a major Canadian SNS site on May 21, and Evernote on June 11.

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the MITF*37, a malware activity observation project operated by IIJ. The MITF uses honeypots*38 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 April 1 and June 30, 2014. 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 demonstrated scanning behavior targeting TCP ports utilized by Microsoft operating systems. We also observed scanning behavior targeting 1433/TCP used by Microsoft's SQL Server, 3389/TCP used by the RDP remote login function for Windows, ICMP echo requests, 22/TCP used for SSH, 53/UDP used for DNS, and 23/TCP used for telnet.

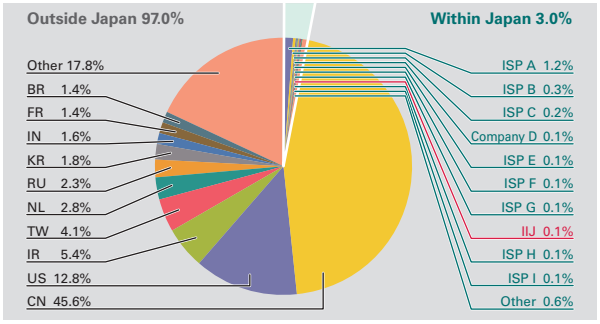


Figure 5: Sender Distribution (by Country, Entire Period under Study)

Communications thought to be SSH dictionary attacks also occurred sporadically during the current survey period. For example, such communications were made from IP addresses allocated to China on April 12, Thailand and China on May 4, and China on June 1. ICMP echo requests detected on April 3 and April 4 involved a group of over 500 IP addresses allocated to China communicating with

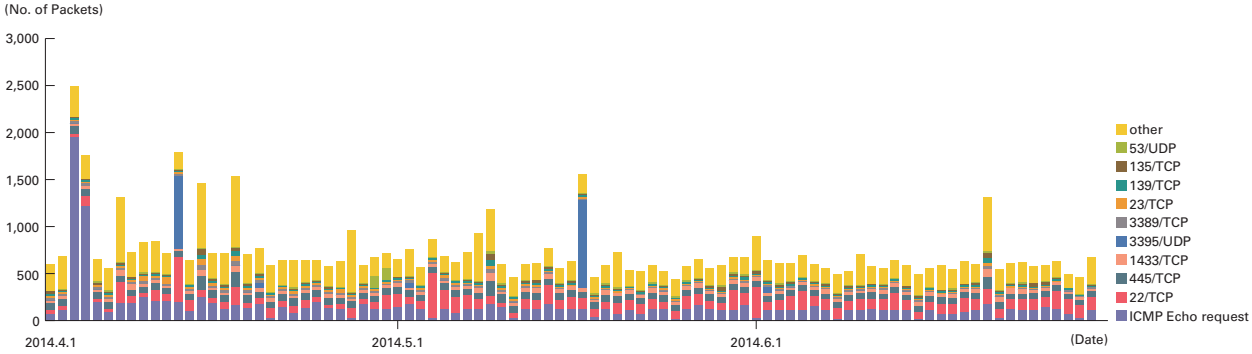


Figure 6: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

*37 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.

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

a single IP address. On April 12 and May 17, communications targeting 3395/UDP were made to the IP address of a specific honeypot from IP addresses allocated to Iran. Upon investigating these communications, we found that random data from several dozen to several hundred bytes in length had been sent.

■ 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*39, while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*40. 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 report, for Figure 8 and Figure 9 we have detected Conficker using multiple anti-virus software packages, and removed any Conficker results when totaling data.

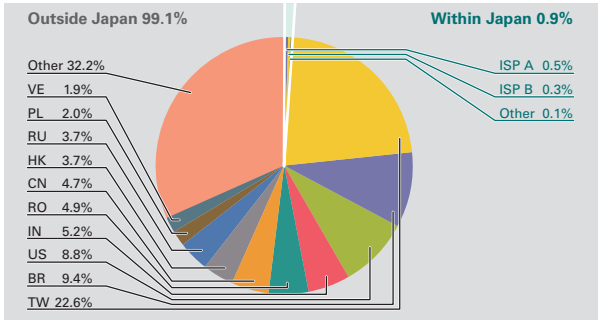


Figure 7: Distribution of Acquired Specimens by Source (by Country, Entire Period under Study, Excluding Conficker)

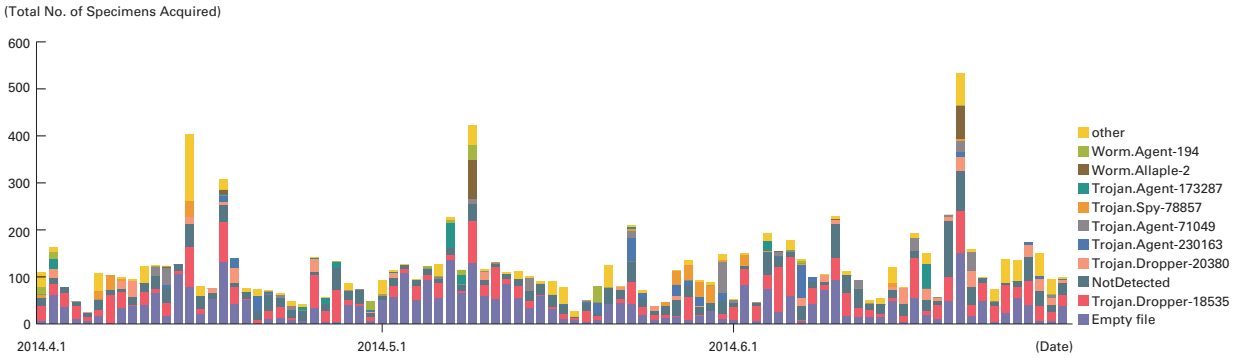


Figure 8: Trends in the Total Number of Malware Specimens Acquired (Excluding Conficker)

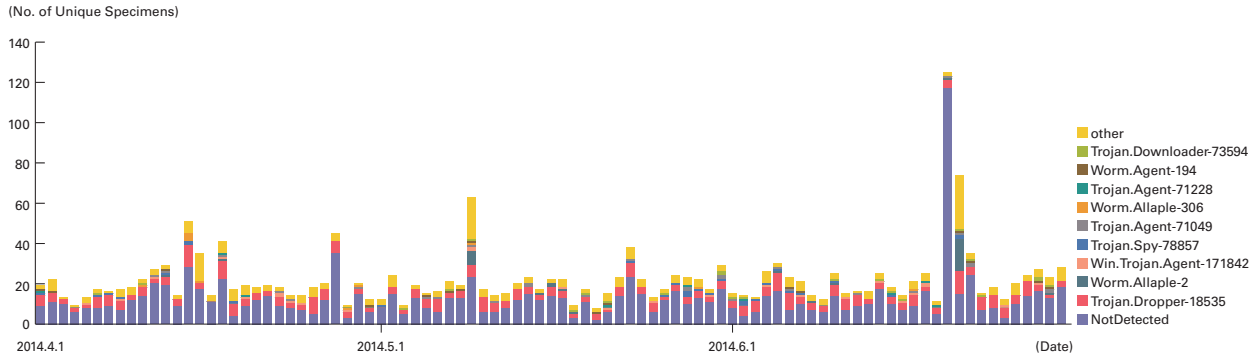


Figure 9: Trends in the Number of Unique Specimens (Excluding Conficker)

*39 This indicates the malware acquired by honeypots.

*40 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.

On average, 121 specimens were acquired per day during the period under study, representing 22 different malware. After investigating the undetected specimens more closely, worms*41 were observed from IP addresses allocated to a number of countries, including the United States, China, and India. Additionally, about 54% 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 94.8% of malware specimens acquired were worms, 1.0% were bots, and 4.2% were downloaders. In addition, the MITF confirmed the presence of 7 botnet C&C servers*42 and 123 malware distribution sites. Although the number of malware distribution sites rose, this is because one of the specimens used DGA.

■ Conficker Activity

Including Conficker, an average of 31,955 specimens were acquired per day during the period covered by this report, representing 718 different malware. While figures rise and fall over short periods, Conficker accounts for 99.6% of the total number of specimens acquired, and 96.9% of unique specimens. This demonstrates that Conficker remains the most prevalent malware by far, so we have omitted it from figures in this report. The total number of specimens acquired during the period covered by this report decreased by approximately 11% compared to the previous survey period. Unique specimens were also down by about 9%. According to the observations of the Conficker Working Group*43, as of June 30, 2014, a total of 1,020,045 unique IP addresses are infected. This indicates a drop to about 32% of the 3.2 million PCs observed in November 2011, but it demonstrates that infections are still widespread.

1.3.3 SQL Injection Attacks

Of the types of different Web server attacks, IIJ conducts ongoing surveys related to SQL injection attacks*44. SQL injection attacks have flared up in frequency numerous times in the past, and remain a major topic in Internet security. SQL injections are known to occur in one of three attack patterns: those that attempt to steal data, those that attempt to overload database servers, and those that attempt to rewrite Web content.

Figure 10 shows the distribution of SQL injection attacks against Web servers detected between April 1 and June 30, 2014. Figure 11 shows trends in the numbers of attacks. These are a summary of attacks detected by signatures on the IIJ Managed IPS Service.

The United States was the source for 35.3% of attacks observed, while China and Japan accounted for 24.6% and 13.1%, respectively, with other countries following in order. There was a slight drop in the number of SQL injection attacks made against Web servers compared to the previous report.

During this period, attacks from multiple attack sources in Europe directed at specific targets took place on May 7. On May 12, attacks from a number of attack sources in China directed at specific targets also took place. On May 25, attacks were made from a number of sources in Europe and China directed at specific targets. On May 30, attacks were observed from multiple sources in Europe and the United States directed at specific targets, along with attacks from specific sources in China on other specific targets. On June 27, a large-scale attack on specific targets from specific attack sources in South Korea and China was observed. These attacks are thought to have been attempts to find vulnerabilities on a Web server.

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.

*41 WORM_ATAK (http://about-threats.trendmicro.com/archiveMalware.aspx?language=jp&name=WORM_ATAK.D).
*42 An abbreviation of Command & Control Server. A server that provides commands to a botnet consisting of a large number of bots.
*43 Conficker Working Group Observations (http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking).
*44 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.

1.3.4 Website Alterations

Here we show the status of website alterations as surveyed through the MITF Web crawler (client honeypot)*45. This Web crawler accesses tens 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.

Angler or Nuclear were behind many of the drive-by download attacks observed between April and June 2014 (Figure 12). Both feature functions for exploiting vulnerabilities in plug-ins such as Java and Flash, but one distinctive feature of Angler is that it also targets Silverlight vulnerabilities (CVE-2013-0074/CVE-2013-3896).

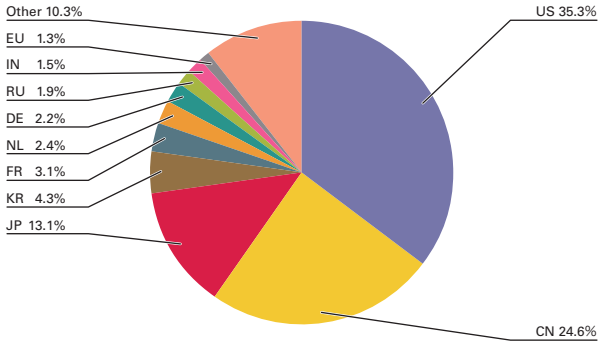


Figure 10: Distribution of SQL Injection Attacks by Source

Small-scale attacks observed included a number of attempts to directly execute malware (exe) in the redirector JavaScript via the Location property without using an exploit kit. Because browsers display a dialog box prompting users to confirm whether or not to execute for this kind of redirection, it is technically not a drive-by download. However, if a user carelessly permits execution, the malware will be executed. We also identified a number of websites altered and used for redirection that had remained in the same state intermittently for over six weeks after their alteration was first observed.

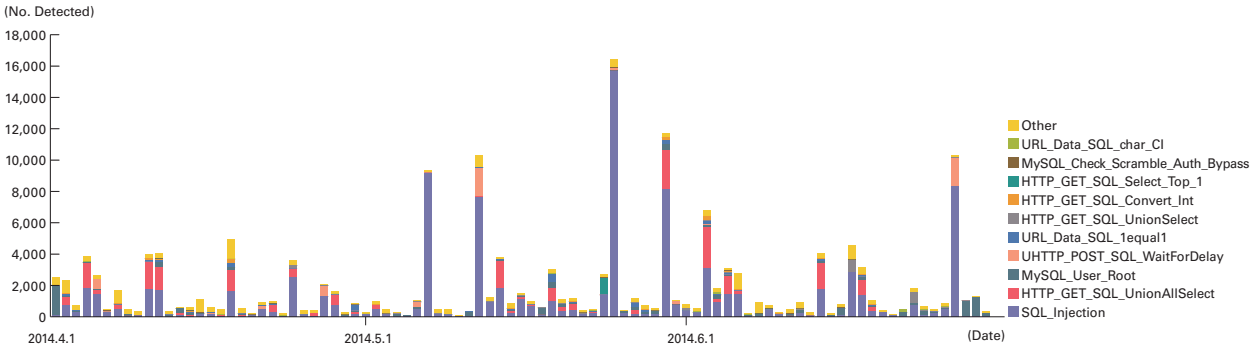
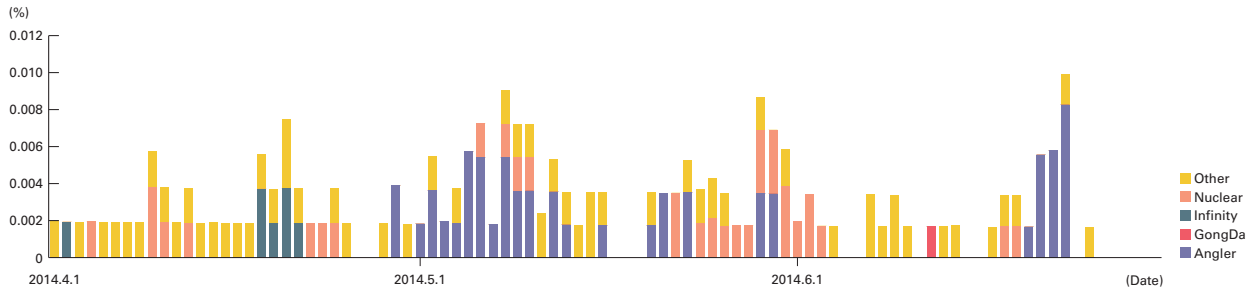


Figure 11: Trends in SQL Injection Attacks (by Day, by Attack Type)



*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.
*Because the Web crawler was not operating between June 26 and June 30, no attacks were detected during that period.

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

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

Overall, it is estimated that the incidence rate for drive-by downloads is still on the decline. However, this trend may abruptly change based on the intentions of attackers, so website operators and visitors must continue to be careful.

1.4 Focused Research

Incidents occurring over the Internet change in type and scope from one minute to the next. Accordingly, IIJ works toward implementing countermeasures by continuing to perform independent surveys and analyses of prevalent incidents. Here, we present information on three topics based on research we have undertaken, including a look at OpenSSL vulnerabilities, and discussion of the "Vawtrak" malware that steals authentication information for financial institutions in Japan. We also examine systems for auditing and confirming the safety of cloud services.

1.4.1 OpenSSL Vulnerabilities

OpenSSL*46 is an open source cryptographic software library implementation that is widely used in Unix environments. There are other implementations with similar functions, for example, GnuTLS*47 and Network Security Services (NSS)*48. For Windows environments, Cryptographic API (CryptoAPI) and Cryptography API Next Generation (CNG) are built in as standard OS functions. These libraries perform the encryption of Web-based and other communications, as well as the processing of server certificates, so they handle highly confidential data. Their most common use is in protecting the confidentiality of Web services. They are utilized in user authentication, as well as during the input of payment information such as credit card details when shopping online.

A number of vulnerabilities in the OpenSSL library and efficient attacks on specific cryptographic algorithms that can be used on SSL/TLS have been disclosed in the past. However, for most of these vulnerabilities a variety of prerequisites had to be met before an attack could be made, and only fragments of information could be gained through a successful attack, so there was hardly any immediate serious impact.

Meanwhile, the recently discovered Heartbleed and CCS Injection vulnerabilities have had a critical impact, with the former allowing private keys and data saved on servers to leak, and the latter allowing encrypted communications to be decrypted. As a result they have drawn significant attention. Both vulnerabilities stem from issues with OpenSSL implementations, rather than problems with specific cryptographic algorithms or the SSL/TLS specifications, so other implementations were not affected by them.

■ About Heartbleed

This vulnerability was disclosed in an OpenSSL security advisory (CVE-2014-0160)*49 released on April 7, 2014. Table 1 shows how it affects each implementation. Only OpenSSL versions 1.0.1 and later were affected in this case. All corresponding versions were affected by the vulnerability, regardless of the combination of client and server implementations involved.

An OpenSSL version of 1.0.1 or later is required to use the TLS v1.1 and TLS v1.2 protocol versions. TLS v1.1 and TLS v1.2 are protocol versions with a range of enhanced security functions, including fixes for previously discovered problems in the specifications, and the addition of strong cryptographic algorithms. This version of OpenSSL was the only one vulnerable, and ironically only the servers that supported new protocol versions for enhanced security were affected. Specifically, an issue with the implementation of heartbeat processing caused parts of the process memory space, which is normally unreadable, to be included in responses when requests containing specially crafted data were sent.

Table 1: List of Implementations Affected by Heartbleed

Implementation	Vulnerabilities
OpenSSL 1.0.1 family	Affected
OpenSSL 1.0.0 family	Not affected
OpenSSL 0.9.8 family	Not affected
Other implementations	Not affected

*46 OpenSSL: The Open Source toolkit for SSL/TLS (http://www.openssl.org/).
*47 The GnuTLS Transport Layer Security Library (http://www.gnutls.org/).
*48 Network Security Services (https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS).
*49 "OpenSSL Security Advisory [07 Apr 2014] TLS heartbeat read overrun (CVE-2014-0160)" (http://www.openssl.org/news/secadv_20140407.txt).

Many vulnerabilities like this that allow the reading of data in memory that usually cannot be accessed have been discovered in the past, in the form of kernel or driver vulnerabilities that only make local attacks possible. However, because the Heartbleed vulnerability is exploitable over networks, allows large amounts of data to be read, and results in no logs being left behind after an attack, it became a serious issue.

The data in memory obtained through an attack depends on the OS, memory allocator, application implementation, and process state, so the target data is not always procured. However, this attack uses non-destructive methods, so it can be attempted any number of times. It has been pointed out that the information obtained could include data not normally disclosed externally, such as private keys stored on the server, or the authentication information of other users.

After this vulnerability was disclosed, CloudFlare held the Heartbleed Challenge*50, which involved using the vulnerability to steal a private key stored on a server. Soon after it began there were a number of reports that the key had been successfully stolen, indicating that the leak of private keys was a realistic threat. It has also been pointed out that even when the private key information is not stolen in its entirety, it could be recovered from partial information*51.

An upgrade to a fixed version is required to deal with this vulnerability, and considering the leak of private keys, it will also be necessary to create new key pairs, reissue certificates using them, and revoke existing certificates. This is because it is difficult to disprove that servers have been attacked in the past, so countermeasures must take in account scenarios in which private keys have already leaked.

■ About CCS Injection

This vulnerability was disclosed in an OpenSSL security advisory (CVE-2014-0224)*52*53 released on June 5, 2014. Versions 0.9.8 and later of OpenSSL are affected, which at the time of disclosure covered all supported versions. Table 2 shows the implementation combinations affected by this vulnerability. The vulnerability only affected combinations of client version 0.9.8 or later and server version 1.0.1 or later.

This vulnerability allowed MITM attacks that could fully decrypt encrypted communications or alter content due to a problem with the processing of Change Cipher Spec messages, which are sent when switching to encrypted communications after SSL/TLS negotiation is complete.

One example of past vulnerabilities that have allowed full decryption in the same way was the issues with SSL v2. Because communications were not protected during negotiation in SSL v2, they could be altered easily. Consequently, it was possible for attackers to forcibly downgrade the cryptographic algorithm used in communications to a weaker one that could be decrypted. This problem was resolved by introducing a system for detecting the alteration of communications during negotiation in SSL v3 and later. However, the Change Cipher Spec messages used in the new vulnerability were not subject to this alteration detection, allowing injections via MITM attacks on OpenSSL implementations.

Table 2: List of Implementations Affected by CCS Injection

		Client Implementation			
Server Implementation		OpenSSL 1.0.1 family	OpenSSL 1.0.0 family	OpenSSL 0.9.8 family	Other implementations
	OpenSSL 1.0.1 family	Affected	Affected	Affected	Not affected
	OpenSSL 1.0.0 family	Not affected	Not affected	Not affected	Not affected
	OpenSSL 0.9.8 family	Not affected	Not affected	Not affected	Not affected
	Other implementations	Not affected	Not affected	Not affected	Not affected

*50 The Heartbleed Challenge (https://www.cloudflarechallenge.com/heartbleed).

*51 We have also examined the recovery of private keys from partial information on the IIJ-SECT blog. IIJ-SECT blog, "The reality of private keys leaking through the Heartbleed bug" (https://sect.iij.ad.jp/d/2014/04/159520.html) (in Japanese).

*52 "OpenSSL Security Advisory [05 Jun 2014] SSL/TLS MITM vulnerability (CVE-2014-0224)" (http://www.openssl.org/news/secadv_20140605.txt).

*53 For more information on this vulnerability and how it was discovered, see the blog of the discoverer, Lepidum Co. Ltd. Lepidum Co. Ltd., see "CCS Injection Vulnerability" (http://ccsinjection.lepidum.co.jp/) and "How the CCS Injection vulnerability (CVE-2014-0224) was discovered" (https://lepidum.co.jp/blog/2014-06-05/CCS-Injection/) (in Japanese).

The processing of Change Cipher Spec messages in OpenSSL differs between servers and clients, even when the same version of OpenSSL is used. This difference is why the affected versions vary depending on where they are used. Because an attack must be made on both the server and client due to the characteristics of the vulnerability, cases in which either of these uses a version that is not vulnerable, or an implementation other than OpenSSL, are not affected. There are other details that determine whether a configuration is affected, and these are also discussed on the IIJ Security Diary site*54.

Unlike Heartbleed, this vulnerability does not cause the leak of private keys saved on a server, etc., so it only requires an upgrade to a fixed version.

■ Summary

When vulnerabilities are discovered in a widely used library like OpenSSL, they have far-reaching effects. Also, because communication that requires encryption often involves important information, the impact is naturally significant.

After the Heartbleed bug became a major problem, the Linux Foundation teamed up with major IT companies to establish the Core Infrastructure Initiative*55, which supports infrastructure-oriented open source projects. The OpenSSL project is an example of a candidate for this support.

The OpenBSD project has also launched the LibreSSL project*56. LibreSSL is a fork of the OpenSSL code aimed at refactoring it and removing unnecessary functions and code to create an implementation focused on security.

Similarly, Google also established the BoringSSL project*57. This is a derivative project tailored for their own software, and is not intended to replace OpenSSL. They will first apply the results to Chromium, on which Chrome is based, with an eye toward expanding use to Android and other areas in the future.

Although these use different approaches, they are all designed to prevent critical issues such as Heartbleed affecting the underlying software again. This demonstrates that software creators are also implementing a variety of countermeasures, but the fact remains that it is difficult to completely eliminate bugs and vulnerabilities. As a result, software users must also stay abreast of vulnerability information that is published, and take appropriate measures when a vulnerability that affects them is disclosed.

1.4.2 The Vawtrak Malware That Steals Authentication Information, etc. for Japanese Financial Institutions

Vawtrak (also known as Neverquest, Snifula, and ZeuS Based Pony, etc.) is malware that is reported to have caused infections overseas since around 2013*58. However, between April and June 2014, it also began to be observed in Japan*59. It features functions for stealing authentication information saved on infected computers or used in online banking, as well as functions for directly manipulating computers from an external source using the VNC protocol. It spread through websites in Japan that had been altered, and IIJ has extracted and analyzed Vawtrak specimens collected through the MITF Web crawler*60. In this section, we present the results of our analysis and discuss countermeasures. The hashes of the specimens in question are shown below.

MD5: 8e8d2a1eafb5c685a02a9adf0890f3bc
SHA-1: 3174ee12fad4422a50655727b0d00222e09239ea
(Dropper)

MD5: aa8422fb8eee6f677cc044212cdd96b9
SHA-1: 7bf386bbf56fbcd16f35e5010f559bbd5cb14634
(after unpacking the 32-bit DLL)

*54 IIJ-SECT blog, "The impact of the OpenSSL vulnerability that allows man-in-the-middle attacks" (https://sect.iij.ad.jp/d/2014/06/069806.html).
*55 Core Infrastructure Initiative (http://www.linuxfoundation.org/programs/core-infrastructure-initiative).
*56 LibreSSL (http://www.libressl.org/).
*57 BoringSSL (https://boringssl.googlesource.com/).
*58 It was first detected by Microsoft's "Malware Protection Center (http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Backdoor:Win32/vawtrak.A)" in May 2013.
*59 In addition to IIJ's observations, a TrendMicro blog post "'VAWTRAK' and 'AIBATOOK': two Internet-based attacks that struck Japan in the last week of May (http://blog.trendmicro.co.jp/archives/9236)" reported a sharp rise in the detection of Vawtrak in Japan, peaking in late May 2014.
*60 See "1.3.4 Website Alterations" in this report for more information about the MITF Web crawler.

Main Functions and Characteristics

One of the key characteristics of Vawtrak is that it features functions that closely resemble ZeuS (a.k.a. Zbot)*61 and Pony (a.k.a. Fareit)*62. Specifically, it is equipped with most of the distinguishing features of ZeuS, such as WebInject*63, DynamicConfig, reporting, a VNC server, and a SOCKS proxy. It also has a function for collecting account information from configuration files saved on the computer for applications such as Web browsers, email clients, FTP clients, and SSH clients. The types of applications targeted by this function are an almost perfect match for those targeted by Pony. The rate of concordance (via BinDiff) between the execution code of the Vawtrak specimen we obtained and ZeuS and Pony was 8% and 20%, respectively. However, because the source code of both ZeuS and Pony has been leaked to the Internet in the past, we think it is likely that many functions have been implemented based on this source code.

Below we explain each function of the specimen in line with the behavioral flow of Vawtrak.

Upon infection, the exe format dropper is the first file executed. Based on the environment it is executed in, this drops a 32-bit or 64-bit dll file with a random file name and the .dat extension into CSIDL_COMMON_APPDATA (C:\ProgramData in the case of Windows Vista, 7, and 8), and modifies the registry to automatically execute it upon startup (Figure 13). It then performs a code injection of the main body of Vawtrak equivalent to the abovementioned dll file into explorer.exe, and deletes itself to finish with.

Although the dropper is deleted, the dropped dll file and the autorun registry entry can be found comparatively easily, so they can be used as indicators of infection with this specimen*64.

The code injected into explorer.exe is also injected into all but a few processes, such as svchost.exe and wininit.exe. When a computer user later launches a browser such as Internet Explorer or Firefox and begins Internet communications, Vawtrak connects to a previously-determined C&C server via HTTP, and downloads the DynamicConfig file containing additional settings, etc. The DynamicConfig is compressed using aPLib*65 and encrypted via a unique method. It is decrypted after download, and also saved to the registry in case of a reboot.

The C&C servers that this specimen connected to are shown below.

baggonally.com	mentilix.com
bennimag.com	humpold.com
sandoxon.com	185.13.32.67
185.13.32.80	146.185.233.38
maxigolon.com	146.185.233.80
terekilpane.com	

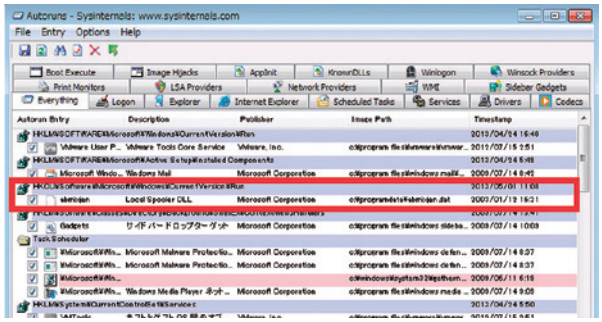


Figure 13: Registry Modified by Vawtrak

*61 See "1.4.3 ZeuS and its Variants" in IIR Vol.16 (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol16_EN.pdf) for more information on ZeuS.

*62 See the IIJ Security Diary "Follow-Up on Alteration Incidents in Japan Exploiting BHEK2" (https://sect.iij.ad.jp/d/2013/03/225209.html) (in Japanese) for a detailed explanation of Pony.

*63 WebInject is a function for altering Web content in browser memory by setting hooks for the Web browser's communication system API. Most banking Trojan malware such as ZeuS and SpyEye have functions like this to deceive a user into entering additional information such as a password for two-factor authentication when the user logs in to a financial institution. The stolen authentication information is used to attempt to misappropriate funds. A detailed explanation of WebInject can be found in IIR Vol.18 (http://www.iij.ad.jp/en/company/development/iir/018.html) under "1.4.2 The Citadel Variant of ZeuS," or IIR Vol.13 (http://www.iij.ad.jp/en/company/development/iir/013.html) under "1.4.2 SpyEye."

*64 Because these values and paths can be changed easily, they may not be usable as indicators for other Vawtrak variants with different configurations, etc.

*65 An open source compression library published by Ibsen Software (http://ibsensoftware.com/products_aPLib.html).

Upon obtaining and analyzing the DynamicConfig, we found it contained URLs for services related to online banking and credit cards, including major financial institutions in Japan, as WebInject targets (Figure 14)*66. Additionally, URLs for well-known SNS and cloud services, video sharing services, and file-sharing services in Japan and abroad were listed as targets for the theft of information when viewed.

Aside from the DynamicConfig mentioned above, Vawtrak also receives the next command for it to carry out from the C&C server. During our analysis, we confirmed the receipt of commands for Vawtrak to upgrade its own version and steal digital certificates saved on the computer. Digital certificate theft is a function for extracting all certificates in the certificate store provided on Windows OSes and sending them to a C&C server. The digital certificates stored on computers have multiple purposes, and when certificates leak there is a risk of impersonation by a third party with regard to each of these.

Vawtrak also features functions not found in ZeuS or Pony, such as those for blocking anti-malware software by abusing Windows OSes' software restriction policies, and those for attempting to disable Rapport*67. Table 3 shows how the features of Vawtrak compare to ZeuS and Pony.

■ Infection Vectors

MITF's Web crawler obtained Vawtrak specimens from multiple websites targeted at Japanese users. The HTML file for the top page of each of the websites in question had been altered, and iframe tags had been inserted without authorization. Website visitors are redirected to an external Web server via these iframe tags, ultimately leading to infection with malware such as Vawtrak through drive-by-download using the Nuclear Exploit Kit or Angler Exploit Kit.

Overseas there have been reports of Vawtrak being distributed via email and other methods*68. In Japan, it is estimated that it spreads mainly through drive-by-downloads via altered websites.

One of the altered websites was for the group company of a well-known content provider in Japan, which was observed in an altered state intermittently from late April to mid-June, and again from mid- to late July. We have been observing a number of websites, including prominent ones such as this, remaining in an altered state for extended periods of time.

*After decryption, a check of the 4 byte "ECFG" string at the beginning (blue box) was performed, so we think this is used as a magic word indicating the beginning of the DynamicConfig. Incidentally, ECFG is believed to be an abbreviation of Extended Config or Encrypted Config. Information in this figure specific to each of the targeted financial institutions has been blacked out.

Figure 14: Part of the DynamicConfig for Vawtrak Obtained (decrypted / red boxes indicate URLs for services such as financial institutions in Japan)

*66 The DynamicConfig files collected at the time of writing this report (August 1 2014) also included additional URLs for a number of regional banks and credit card companies.

*67 Rapport is anti-malware software developed by Trusteer that is tailored to countering threats to online banking, such as Web injections and phishing (http://www.trusteer.com/ja/products/trusteer-rapport-for-online-banking-ja) (in Japanese). Trusteer stated in a blog post titled "Carberp's Attempt to Bypass Trusteer Rapport is Effectively Resisted (http://www.trusteer.com/blog/carberps-attempt-to-bypass-trusteer-rapport-is-effectively-resisted)" that Rapport was not affected as intended by a mechanism in malware known as Carberp that attempts to bypass it like Vawtrak.

*68 For example, a post on the Kaspersky Lab blog titled "Online Banking Faces a New Threat" (http://securelist.com/blog/57881/online-banking-faces-a-new-threat/) states that infections were being spread through spam.

Countermeasures

To prevent malware infections through drive-by-downloads, it is important to always keep the OS, browser, and related plug-ins on a client PC up-to-date, and free of vulnerabilities. When the client OS is Windows, it is also effective to use software restriction policies to limit the executable area for programs, and install EMET to mitigate the effect of vulnerabilities*69.

In the event that a Vawtrak infection occurs, it will be necessary to restore the computer by performing a clean install, revoke digital certificates that were used, and change the passwords used through client applications on the computer. Additionally, if Web services such as online banking or SNS were used on the computer in question, the account information and details exchanged over those services may have leaked, so appropriate measures such as changing or deleting this information must be taken.

Meanwhile, website operators and administrators should bear in mind that they have a responsibility to do their utmost to prevent sites from being altered and used as exploit kit redirection sources. It is necessary to have a comprehensive understanding of the systems used, including Web servers, content management systems and their plug-ins, or frameworks these depend on. They must also be managed in a way that prevents them from being affected by attacks on vulnerabilities. There have also been cases in which website visitors have been exposed to the threat of malware infections due to security breaches at external resources such as CDN, advertisement services, and access analysis services, which are involved with the company's website*70. Threats that stem from external systems such as these cannot be eliminated by merely performing repeated diagnosis of your system and improving its protection. Although it depends on the nature of the service provided, with regard to external resources whose integrity cannot be assured, we recommend you consider moving them in-house or discontinuing them according to their importance. When continuing to use external resources after evaluating this, we encourage you to regularly view your website from an external client and check the content actually downloaded to the client PC, to detect any problems directly as soon as possible.

1.4.3 Cloud Security Confirmation and Audit Systems

Here we take a look at use of the various guides published to enable users to utilize cloud services safely. We also discuss the "Cloud Information Security Audit System" being evaluated by the Cloud Information Security Promotion Alliance.

Table 3: Characteristic Vawtrak Functions and Comparison with Zeus and Pony

	vawtrak	Zeus (2.0.8.9)	Pony (1.9)	Notes
Acquisition of authentication information saved on PCs	✔	✔	✔	The client applications targeted by Vawtrak and Pony 1.9 (about 100 in total) are almost identical. ZeuS targets around 20, and the types are also different. There are no matches with Pony 2.0.
Acquisition of digital certificate information saved on PCs	✔	✔	✔	
DynamicConfig	✔	✔		Different configuration formats.
WebInject	✔	✔		
Obfuscation of internal strings	✔	✔		
Report function	✔	✔		
SOCKS proxy	✔	✔		
VNC server	✔	✔		
32-bit / 64-bit support	✔			
Blocks anti-malware software using software restriction policies	✔			
Attempted disabling of Rapport	✔			

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

*70 For example, the following Symantec Security Response blog post gives a detailed explanation of incidents in which legitimate websites that used CDN services were compromised and exploited. "Recent Exploit for Adobe Flash Vulnerability Targeting Users in Japan for Financial Information" (http://www.symantec.com/connect/blogs/recent-exploit-adobe-flash-vulnerability-targeting-users-japan-financial-information).

■ Cloud Security Guides

Eight years have already passed since the concept of cloud computing was introduced in 2006. Since then, a range of services using cloud computing technology (henceforth "cloud services") have been introduced, and are now widely used by the public. However, since the inception of cloud services various doubts have been cast regarding their safety, and security concerns have been the top obstacle to adopting them. In fact, large-scale information security incidents both in Japan and abroad are still fresh in our minds. Subsequently, through various discussions, information including guides for safely providing and using cloud services has now been published by a number of organizations. Table 4 lists examples of these guides, and provides an overview of them.

As mentioned above, guides regarding cloud security have been issued by a range of organizations and groups. Although the large number of guides makes it harder to select the best guide for your purposes, we should welcome the fact that information is now much easier to obtain than in the past.

■ Points to Note When Using Guides

These guides contain many useful pieces of information regarding security issues that should be considered when using or providing cloud services, and they are also commonly used as checklists. However, the guides can be interpreted in a number

Table 4: Samples Guides for Providing/Using Cloud Services Safely

Title	Issuing Organization	Date of Issue	Overview
Information Security Guidelines for Cloud Services*71	Ministry of Internal Affairs and Communications	April 2014	A guide mainly targeting cloud service providers that summarizes points such as how information security measures should be implemented and what kind of information should be disclosed from a practical perspective.
Guide for Protecting Cloud Service Users and Ensuring Compliance*72	ASP-SaaS-Cloud Consortium	July 2011	Explains points to consider for conducting appropriate risk management when companies in particular use public cloud services.
System for Certifying the Disclosure of Information Pertaining to IaaS/PaaS Security/Reliability*73	Foundation for MultiMedia Communications	August 2012	A system for certifying that IaaS/PaaS providers are appropriately disclosing information about security/reliability. The System for Certifying the Disclosure of ASP/SaaS and Data Center Information is another similar system.
Information Security Management Guidelines for the Use of Cloud Services*74	Ministry of Economy, Trade and Industry	Published April 2011, revised March 2014	Prescribes standards for cloud service security management based on ISO/IEC27002. It is mainly targeted at users, but it also covers topics such as how providers should respond to user requests.
Security Measure Standards/Handbook for Computer Systems at Financial Institutions (Supplement to Eighth Revision)*75	The Center for Financial Industry Information Systems	March 2013	A document that incorporates points that should be considered when using cloud services into previous security guidelines for financial institutions. It contains information about risk assessment when financial institutions use cloud services.
CSA Cloud Control Matrix (CCM)*76	Cloud Security Alliance	July 2014 V3.0.1	Summarizes the controls listed in the "Cloud Security Guidance" issued by CSA, as well as policies for their implementation. The controls listed in CCM are also mapped to various other standards.
ISO/IEC CD 27017 Information technology -- Security techniques -- Code of practice for information security controls for cloud computing services based on ISO/IEC 27002*77	International Organization for Standardization (ISO)	Publication planned for October 2015	International standards for cloud security that are currently being under discussion. They are based on ISO/IEC 27002, with the addition of controls required by users and providers for implementing cloud security.

*71 Ministry of Internal Affairs and Communications, "Information Security Guidelines for Cloud Services" (http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/140402_01.html).

*72 ASP-SaaS-Cloud Consortium, "Guide for Protecting Cloud Service Users and Ensuring Compliance" (http://aspicjapan.org/information/guideline/pdf/jp_ver1.0.pdf) (in Japanese).

*73 Foundation for MultiMedia Communications, "System for Certifying the Disclosure of Information Pertaining to IaaS/PaaS" (http://www.fmmc.or.jp/ip-nintei/) (in Japanese).

*74 Ministry of Economy, Trade and Industry, "Information Security Management Guidelines for the Use of Cloud Services" First Edition (http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html) (in Japanese). March 2014 Revised Edition and guidelines (http://www.meti.go.jp/press/2013/03/20140314004/20140314004.html) (in Japanese).

*75 Center for Financial Industry Information Systems, "Security Measure Standards/Handbook for Computer Systems at Financial Institutions (Supplement to Eighth Revision)" (https://www.fisc.or.jp/publication/disp_target_detail.php?pid=266) (in Japanese).

*76 Cloud Security Alliance, "CSA CCM" (https://cloudsecurityalliance.org/research/ccm/). The Japanese version is (http://www.cloudsecurityalliance.jp/ccm_wg.html).

*77 International Organization for Standardization, "ISO/IEC CD 27017 Information technology -- Security techniques -- Code of practice for information security controls for cloud computing services based on ISO/IEC 27002" (http://www.iso.org/iso/catalogue_detail.htm?csnumber=43757).

of ways when the target audience (users or providers) and subject (services or information) is not clear, increasing the risk of misunderstandings or confusion.

For example, "privileged accounts" could be interpreted as "accounts used by a cloud service provider for overall service maintenance (1)," "privileged accounts for the information system section of the service provider (2)," "the root (administrator) account of the virtual machine a user is using via IaaS (3)," or "accounts for conducting maintenance such as the registration or deletion of users via SaaS (4)." If the guide referenced is aimed at users, "privileged accounts" would refer to (3) or (4), while in guides targeting providers this would indicate (1) or (2). Because the implications of checklist questions vary based on different interpretations, there is a risk that proper risk assessment or service use will not be possible.

One method for performing proper risk assessment is to clarify the target audience and subject so that providers and users have a common understanding. For example, clarifying (from either user or provider) that "privileged accounts" are accounts for maintaining the service used, so that everyone is on the same page. Because communication takes place between the provider and user, time and effort are required, but this reduces perception gaps and false assumptions. On the other hand, this hinders the automation that is a feature of cloud services, so not all providers will be able to respond to individual queries like this.

Another method is to search for information disclosed by providers and use it as-is. Because each provider releases some form of information regarding the kind of security features provided and the security measures taken, users can use this published information to decide for themselves whether the level of security they require can be maintained. This method is often seen in typical cloud services. However, while it is not time-consuming or difficult, the information that providers can disclose and its granularity vary, so it may not be possible to get the information you were looking for, and it may be difficult to confirm the reliability of responses.

Another method is to use reports such as SSAE16. Providers only disclose information to external auditors, and users are able to obtain a trustworthy evaluation of a provider's organization from a third party. This method has benefits for both users and providers, but because the external auditor must have an extremely high level of IT knowledge, and the provider ends up paying a higher cost (eventually leading to higher service fees), it is difficult to apply it to cloud services broadly.

An initiative has started that enables cloud providers to evaluate security based on common standards and disclose trustworthy information. This method resolves these various issues, enabling proper risk assessment to be carried out. We will discuss this initiative next.

■ Cloud Information Security Audit System

Cloud services involve large numbers of users utilizing systems prepared by the service provider for the joint use of resources in a set manner. Consequently, unlike system integration, a dedicated system environment is not built for the user, and the details of configurations and operational structures are not made known. Also, because cloud service environments change dynamically, there is no point to guessing at their inner workings. Even if money is spent on carrying out an audit, providers will not reveal the entirety of their system to users. The use of cloud services as a "black box" is unavoidable. That is one reason why security and risk assessment concepts based on conventional on-premise corporate systems are difficult to apply to cloud services.

In light of this, 25 companies including providers involved with cloud services came together under the leadership of the Japan Information Security Audit Association (henceforth "JASA") in April 2013, and founded the "JASA - Cloud Information Security Promotion Alliance (henceforth "J-CISPA)." In September 2012 JASA published its "Cloud Information Security Management Standards," which are based on conventional information security audit systems applied to cloud computing. They intend to provide users with information for carrying out appropriate risk management by performing system audits tailored to cloud services that are rooted in these standards. This trial is a world first, and based on the knowledge gained through these activities J-CISPA is also actively making proposals for the ISO27017 and ISO27036-4 international standards for cloud security that are currently under discussion.

Here we will explain the audit system, shown in Figure 15, that is envisaged by J-CISPA.

J-CISPA has determined the typical risks of concern with regard to cloud services (Table 5). First, a cloud provider clarifies and documents how they handle each of these risks. This is called an "assertion." Figure 16 shows a sample assertion IIJ put together for a pilot audit (detailed later). Next, an internal auditor with auditor qualifications determined by JASA audits the content of the assertion and records the results. The internal auditor conducts the audit using auditing procedures specified in the cloud internal auditing standard procedures put together by JASA's expert working group. Because the content and procedures for the audit are defined in detail, the audit quality is not affected even when a different auditor is used. Using common audit standards also makes it easier to compare how risk is dealt with, even when the provider or service differs.

This system requires an internal auditor to carry out the audit. Because cloud service systems are still developing, and change from moment to moment, it is difficult for anyone other than a specialist with seasoned knowledge of IT technology to determine whether the audit data is correct. The internal auditor of a service provider is able to make decisions based on their accurate knowledge of the service, and this also helps ensure a certain level of audit quality. Additionally, because cloud providers don't need to release confidential information about their service, the burden on them is lessened.

However, even when the audit is carried out by a certified internal auditor using set procedures, from the user's perspective this still amounts to a mere self-assertion. To remedy this, the audit system incorporates an external audit that makes effective use of the results produced by the internal auditor. More specifically, an external auditor verifies whether the internal audit was carried out according to the correct procedures based on the "internal audit report" and other documents obtained through the internal audit. Because the internal audit produces a technically sound audit report with uniform procedures and format is produced, the external audit only needs to audit whether or not the internal audit was carried out correctly.

This audit system incorporates the two-step structure in an attempt to enable an accurate assessment of technical information related to cloud services, along with accurate auditing procedures, at the lowest possible cost. By keeping costs down, more cloud services can support this system. J-CISPA issues marks based on the results, with a silver mark for an assertion of which an internal auditor has carried out an audit, and a gold mark when an external auditor has verified these results. In fiscal 2013, the cloud service providers in the alliance conducted "pilot audits" to trial this system. This fiscal year enthusiastic preparations are underway to conduct actual audits based on the earlier results.

IIJ will continue to actively promote new systems such as this and the creation of domestic and international rules to facilitate the safe use of cloud services.

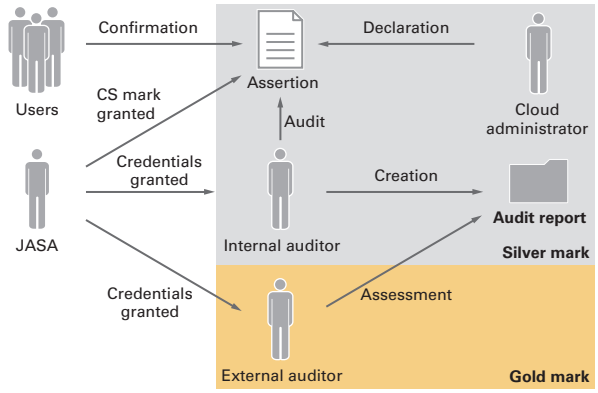


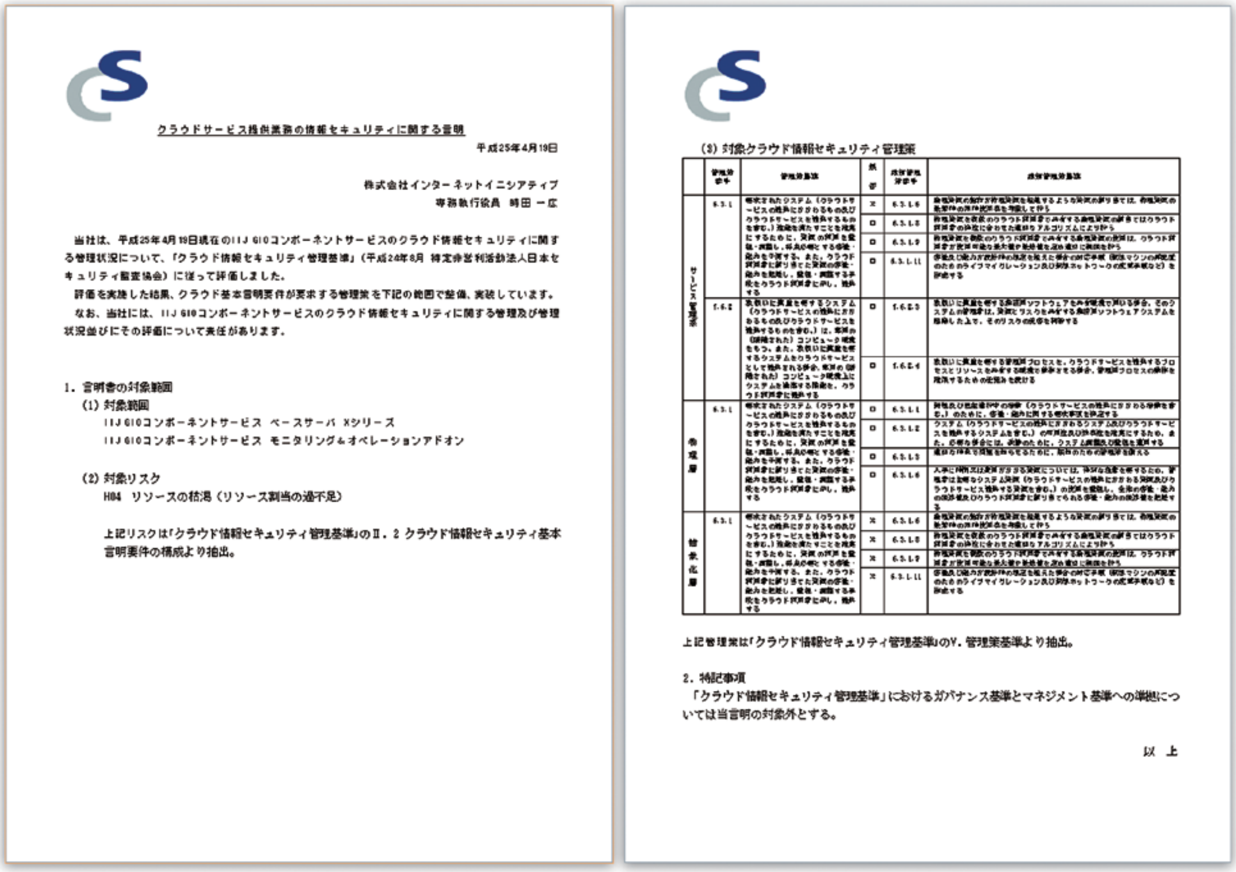
Figure 15: Individual Roles During a Cloud Security Audit

Table 5: Risks of Concern Regarding Cloud Services (taken from J-CISPA materials)

Risk Severity	Number	Risk Identifier
High	H01	Impacts increased due to highly aggregated computing resources and infrastructures
	H02	Mismatches between virtual and physical systems in design and operation phase
	H03	Loss of business reputation due to co-tenant activities
	H04	Resource exhaustion (under or over provisioning)
	H05	Isolation failure
	H06	Compromise of service engine
Medium	M07	Cloud provider malicious insider - abuse of high privilege access
	M08	Management interface compromise (manipulation, availability of infrastructure)
	M09	Intercepting data in transit or data leakage on up/download, intra-cloud
	M10	Insecure or ineffective deletion of data
	M11	DDoS/DoS attacks on cloud
Low	L12	Lock-in
	L13	Loss of governance
	L14	Supply chain failure
	L15	Economic denial of service (EDoS)
	L16	Loss of encryption keys
	L17	Undertaking malicious probes or scans
	L18	Subpoena and e-discovery
	L19	Risk from changes of jurisdiction
	L20	Data protection risks
	L21	Licensing risks

1.5 Conclusion

This report has provided a summary of security incidents to which IIJ has responded. In this report, we provided a summary of OpenSSL vulnerabilities, and looked at the "Vawtrak" malware that steals authentication information, etc. for financial institutions in Japan. We also examined the confirmation of cloud security and audit systems. 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. IIJ will continue striving to provide the necessary countermeasures to allow the safe and secure use of the Internet.



クラウドサービス提供業務の情報セキュリティに関する言明

平成25年4月19日

株式会社インターネットイニシアティブ
専務執行役員　時田 一広

当社は、平成25年4月19日現在のIIJ GIOコンポーネントサービスのクラウド情報セキュリティに関する管理状況について、「クラウド情報セキュリティ管理基準」（平成24年8月 特定非営利活動法人日本セキュリティ監査協会）に従って評価しました。
評価を実施した結果、クラウド基本言明要件が要求する管理策を下記の範囲で整備、実装しています。
なお、当社には、IIJ GIOコンポーネントサービスのクラウド情報セキュリティに関する管理及び管理状況並びにその評価について責任があります。

1. 言明書の対象範囲
(1) 対象範囲
IIJ GIOコンポーネントサービス ベースサーバ Xシリーズ
IIJ GIOコンポーネントサービス モニタリング＆オペレーションアドオン

(2) 対象リスク
H04 リソースの枯渇（リソース割当の過不足）

上記リスクは「クラウド情報セキュリティ管理基準」のII．2 クラウド情報セキュリティ基本言明要件の構成より抽出。

(3) 対象クラウド情報セキュリティ管理策

[illegible]

上記管理策は「クラウド情報セキュリティ管理基準」のV．管理策基準より抽出。

2. 特記事項
「クラウド情報セキュリティ管理基準」におけるガバナンス基準とマネジメント基準への準拠については当言明の対象外とする。

以　上

Figure 16: Sample Assertion for Pilot Audit

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)
Tadashi Kobayashi (1.4.1 OpenSSL Vulnerabilities)
Hisao Nashiwa, Hiroshi Suzuki (1.4.2 The Vawtrak Malware That Steals Authentication Information, etc. for Japanese Financial Institutions)
Masahiko Kato (1.4.3 Cloud Security Confirmation and Audit Systems)
Office of Emergency Response and Clearinghouse for Security Information, Service Operation Division, IIJ

Contributors:
Masafumi Negishi, Yuji Suga, Takahiro Haruyama, Minoru Kobayashi, Yasunari Momoi
Office of Emergency Response and Clearinghouse for Security Information, Service Operation Division, IIJ

Traffic Volumes Rise Steadily Over the Past Year, and HTTPS Use Expands

Looking at broadband traffic over the past year, we can see that traffic volumes have increased steadily, with download volumes up 27%, and upload volumes up 13%.
Also, due to elevated awareness of the importance of protecting privacy there was a shift toward the use of HTTPS in Web traffic that accounts for the majority of traffic. We expect the ratio of HTTPS usage to continue to increase in the future.

2.1 Overview

In this report we analyze traffic over the broadband access services operated by IIJ every year and present the results[*1][*2][*3][*4][*5]. We once again report on changes in traffic trends over the past year based on daily user traffic and usage by port.

Figure 1 shows average monthly traffic across IIJ's entire suite of broadband services for the past seven years, with the maximum value normalized as 1. The drop in traffic in January 2010 is believed to be caused by the amended Copyright Act that came into effect that month, making the download of copyright infringing content illegal. Since then, download volumes (OUT) have continued to rise, while upload volumes (IN) have remained mostly level, indicating that the ratio of P2P file sharing traffic has decreased. In October 2012, a slight increase followed by a decrease was observed when an amended Copyright Act that incorporated criminal punishment for illegal downloads came into effect. Subsequently, download volumes have grown to higher levels than before, and upload volumes are also increasing slowly but steadily. Over the past year IN traffic has increased by 13%, while OUT traffic has increased by 27%.

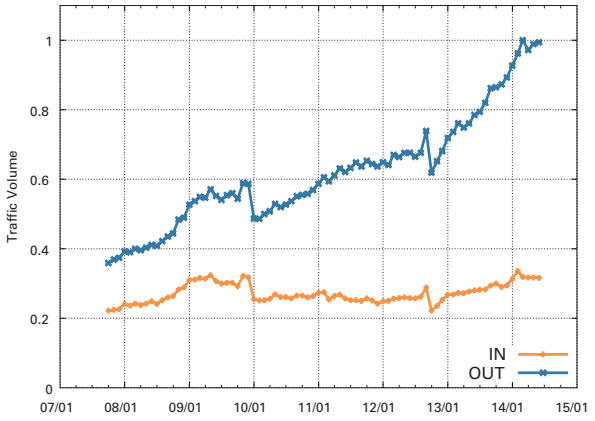


Figure 1: Broadband Traffic Volume Trends for the Past 7 Years

2.2 About the Data

As with our previous reports, the survey data utilized here was collected using Sampled NetFlow from the routers accommodating fiber-optic and DSL broadband customers of our personal and enterprise broadband access services. Because broadband traffic trends differ between weekdays and weekends, we analyze a full week of traffic. In this case, we compare data for the week spanning May 26 to June 1, 2014 with the data we analyzed in the previous report for the week spanning June 3 to June 9, 2013.

The usage volume for each user was obtained by matching the IP address assigned to users with the IP addresses observed. We collected statistical information by sampling packets using NetFlow. The sampling rate was set to 1/8192, taking into

*1 Kenjiro Cho. Broadband Traffic Report: The Impact of Criminalization of Illegal Downloads was Limited. Internet Infrastructure Review. Vol.20. pp32-37. August 2013.
*2 Kenjiro Cho. Broadband Traffic Report: Traffic Trends over the Past Year. Internet Infrastructure Review. Vol.16. pp33-37. August 2012.
*3 Kenjiro Cho. Broadband Traffic Report: Examining the Impact of the Earthquake on Traffic on a Macro Level. Internet Infrastructure Review. Vol.12. pp25-30. August 2011.
*4 Kenjiro Cho. Broadband Traffic Report: Traffic Shifting away from P2P File Sharing to Web Services. Internet Infrastructure Review. Vol.8. pp25-30. August 2010.
*5 Kenjiro Cho. Broadband Traffic: Increasing Traffic for General Users. Internet Infrastructure Review. Vol.4. pp18-23. August 2009.

account router performance and load. We estimated overall usage volumes by multiplying observed volumes by the reciprocal of the sampling rate. Due to the sampling method used there are slight estimation errors in data for low-volume users. However, for users with usage above a certain level we were able to obtain statistically meaningful data.

IIJ provides both fiber-optic and DSL access for its broadband services. However, fiber-optic access now makes up the vast majority of use, with 95% of users observed in 2014 using fiber-optic connections, accounting for 97% of overall traffic volumes.

The IN/OUT traffic presented in this report indicates directions from an ISP's perspective. IN represents uploads from users, and OUT represents user downloads.

2.3 Daily Usage Levels for Users

First, we will examine the daily usage volumes for broadband users from several perspectives. Daily usage indicates the average daily usage calculated from a week's worth of data for each user.

Figure 2 shows the average daily usage distribution (probability density function) per user. It compares data for 2013 and 2014 divided into IN (upload) and OUT (download), with user traffic volume on the X axis, and user frequency on the Y axis. The X axis shows volumes between 10 KB (10^4) and 100 GB (10^{11}) using a logarithmic scale. Some users are outside the scope of the graph, but most fall within the 100 GB (10^{11}) range.

The IN and OUT distribution shows almost log-normal distribution, which looks like a normal distribution in a semi-log graph. A linear graph would show a long-tailed distribution, with the peak close to the left end and a slow decay towards the right. The OUT distribution is further to the right than the IN distribution, indicating that the download volume is more than an order of magnitude larger than the upload volume. Comparing 2013 and 2014, the peak distribution for both IN and OUT traffic has moved slightly to the right, demonstrating that overall user traffic volumes are increasing. The shift is greater than when 2012 and 2013 were compared last year, indicating that traffic volumes have increased at a higher rate.

Looking at OUT distribution, the peak has been steadily moving to the right over the past few years. However, the usage levels of heavy users on the right end have not increased much, and the distribution is beginning to lose its symmetry. Meanwhile, the tail of the IN distribution to the right has grown longer. Previously, both IN and OUT showed a clearer peak here, indicating heavy users with symmetrical IN/OUT volumes. For convenience, we labeled users with asymmetrical IN/OUT traffic distribution that make up the majority "client-type users," and the distribution of heavy users with symmetrical IN/OUT traffic that make up the minority on the right side "peer-type users." In this report we will continue to use these conventions. Over the past few years, the peak for peer-type users has shrunk to the point where it can hardly be distinguished. This indicates that the ratio of heavy users is decreasing. The small spikes on the left of the graph are noise caused by the sampling rate. These correspond to the minimum and maximum packet sizes when only one packet is observed.

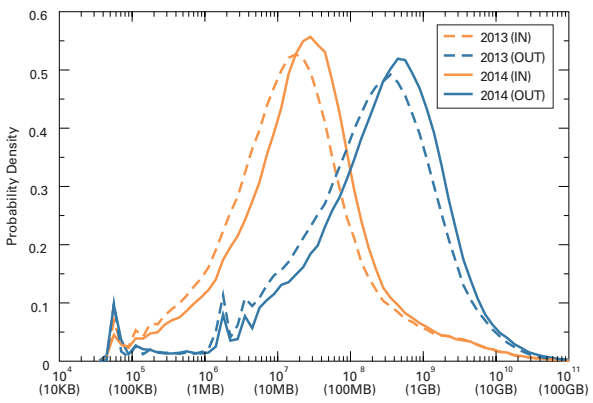


Figure 2: Daily User Traffic Volume Distribution Comparison of 2013 and 2014

	IN (MB/day)		OUT (MB/day)	
Year	Average Value	Most Frequent Value	Average Value	Most Frequent Value
2005	430	3.5	447	32
2007	433	4	712	66
2008	483	5	797	94
2009	556	6	971	114
2010	469	7	910	145
2011	432	8.5	1,001	223
2012	410	14	1,026	282
2013	397	18	1,038	355
2014	437	28	1,287	447

Table 1: Trends in Average Daily Traffic Volume for Users and Most Frequent Values

Table 1 shows trends in the average value and most frequent value that represents peak distribution. Comparing the most frequent values in 2013 and in 2014, IN rose from 18 MB to 28 MB, and OUT rose from 355 MB to 447 MB. This demonstrates that, particularly in the case of downloads, the traffic volume for each user has increased. Meanwhile, because average values are pulled up by the heavy users to the right of the graph, they are significantly higher than the most frequent values, with the average IN value 437 MB and the average OUT value 1,287 MB in 2014. The average values for 2013 were 397 MB and 1,038 MB, respectively. The IN value that had been falling since 2010 has begun to recover, and it seems that the migration from P2P file sharing applications to Web services has settled down.

Figure 3 plots the IN/OUT usage volumes for 5,000 randomly sampled users. The X axis shows OUT (download volume) and the Y axis shows IN (upload volume), with both using a logarithmic scale. Users with identical IN/OUT values are plotted on the diagonal line.

The cluster below the diagonal line and spread out parallel to it represents general client-type users with download volumes an order of magnitude higher than upload volumes. Previously there was a clearly-recognizable cluster of peer-type heavy users spread out thinly on the upper right of the diagonal line, but this is now no longer discernible. Though we have separated client-type and peer-type users for convenience, in actual fact client-type general users also use peer-type applications such as Skype, and peer-type heavy users also use download-based applications on the Web, blurring the boundary between them. In other words, many users use both types of applications in varying ratios. There are also differences in the usage levels and IN/OUT ratio for each user, pointing to the existence of diverse forms of usage. In this respect, almost no difference can be seen between the current data and that for 2013.

Figure 4 shows the complementary cumulative distribution of the daily traffic volume for users. This indicates the percentage of users with daily usage levels greater than the X axis value on the Y axis in a log-log scale, which is an effective way of examining the distribution of heavy users. The right side of the graph falls linearly, showing a long-tailed distribution close to power-law distribution. In any case, it can be said that heavy users are distributed statistically, and are by no means a special class of user.

Figure 5 shows the deviation in traffic usage levels between users. It indicates that users with the top X% of usage levels account for Y% of the total traffic volume. There is a great deal of deviation in usage levels, and as a result traffic volume for a small portion of users accounts for the majority of the overall traffic. For example, the top 10% of

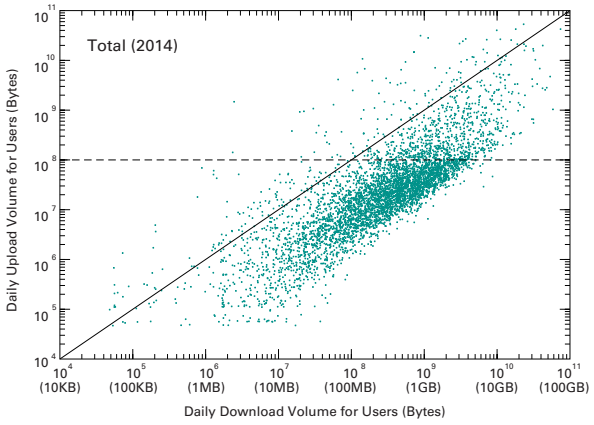


Figure 3: IN/OUT Usage for Each User

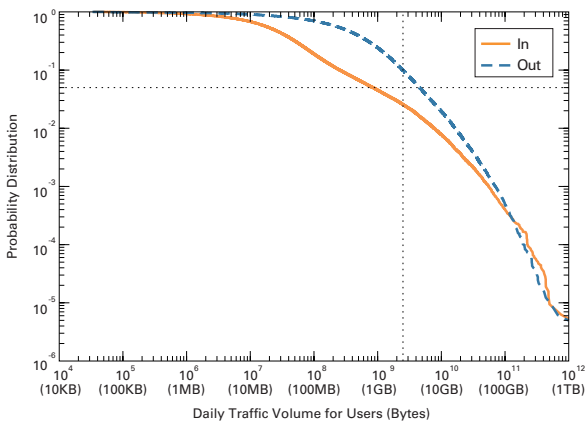


Figure 4: Complementary Cumulative Distribution of the Daily Traffic Volume for Users

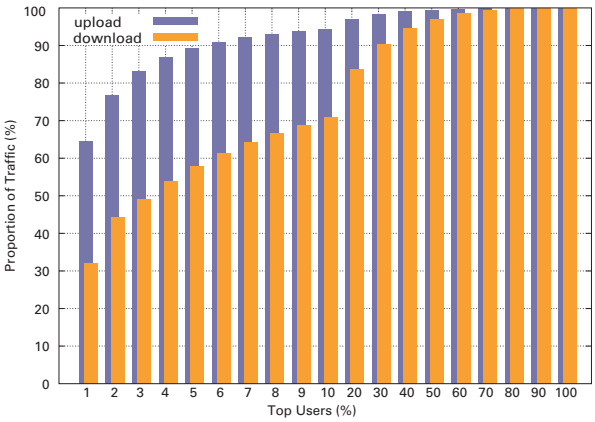


Figure 5: Traffic Usage Deviation between Users

users make up 68% of the total OUT traffic, and 93% of the total IN traffic. Furthermore, the top 1% of users make up 30% of the total OUT traffic, and 65% of the total IN traffic. Along with the decrease in the ratio of heavy users over the past few years, the distribution bias is also dropping slightly.

2.4 Usage by Port Overview

Next, we will look at a breakdown of traffic and examine usage levels by port. Recently, it has been difficult to identify applications by port number. Many P2P applications use dynamic ports on both ends, and a large number of client/server applications utilize port 80 assigned to HTTP to avoid firewalls. To broadly categorize, when both parties use a dynamic port higher than port 1024, there is a high possibility of it being a P2P application, and when one party uses a well-known port lower than port 1024, it is likely to be a client/server application. In light of this, here we will look at usage levels for TCP and UDP connections by taking the lower port number of the source and destination ports.

As overall traffic is dominated by peer-type heavy user traffic, to examine trends for client-type general users, we have taken the rough approach of extracting data for users with a daily upload volume of less than 100 MB, and treating them as client-type users. This corresponds to users below the horizontal line at the IN=100 MB point in Figure 3.

Figure 6 shows an overview of port usage, comparing all users and client-type users for 2013 and 2014. Table 2 shows detailed numeric values for this figure.

80% of traffic in 2014 is TCP based. The ratio of port 80 HTTP traffic was up slightly from 43% in 2013 to 45% this year. The ratio of port 443 HTTPS traffic has also climbed from 4% to 9%. TCP dynamic ports, which have been on the decline, fell from 30% in 2013 to 24% in 2014. The ratio of individual dynamic port numbers is tiny, with port 1935 used by Flash Player the highest at 2% of the total, and the next highest under 0.5%. Almost all traffic other than TCP is related to VPN.

Looking exclusively at client-type users, port 80 traffic that accounted for 82% of the total in 2013 has fallen for the first time, dropping to 75% in 2014. Instead, the ratio for port 443 HTTPS traffic, which is the second highest, rose from 5% in 2013 to 14%. The ratio of dynamic ports also decreased from 9% to 7%.

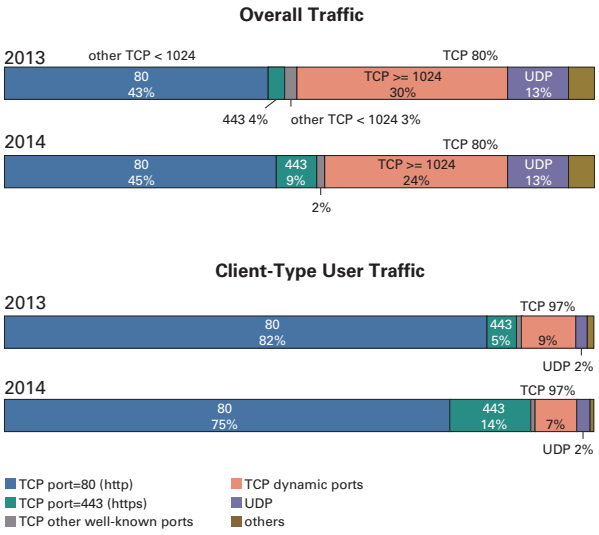


Figure 6: Usage by Port Overview

protocol port	2013		2014	
	total (%)	client type	total (%)	client type
TCP	**79.79**	**96.91**	**80.15**	**97.38**
(< 1024)	49.57	88.15	56.33	90.08
80(http)	43.44	81.61	44.87	74.81
443(https)	3.90	4.80	9.25	13.78
554(rtsp)	0.51	0.58	0.36	0.25
22(ssh)	0.24	0.04	0.31	0.03
(>= 1024)	30.22	8.76	23.82	7.30
1935(rtmp)	2.39	3.60	2.48	4.00
8080	0.34	0.19	0.40	0.17
7144(peercast)	0.40	0.04	0.32	0.02
UDP	**13.21**	**2.12**	**12.51**	**1.81**
ESP	**6.54**	**0.88**	**6.86**	**0.74**
IP-ENCAP	**0.13**	**0.00**	**0.24**	**0.00**
GRE	**0.20**	**0.06**	**0.20**	**0.04**
ICMP	**0.02**	**0.02**	**0.02**	**0.02**
IPv6	**0.01**	**0.01**	**0.01**	**0.00**
L2TP	**0.09**	**0.00**	**0.00**	**0.00**

Table 2: Usage by Port Details

The growth in the use of HTTPS is due to more and more services making regular use of encrypted HTTPS communications since the existence of a U.S. National Security Agency (NSA) program for intercepting communications stirred up controversy in June 2013. Looking at HTTPS traffic volumes broken down by provider for 2014, 59% of the total (67% when isolating client-type users) is related to Google, demonstrating their efforts to proactively adopt HTTPS. Other companies such as Akamai, Amazon, Facebook, Microsoft, and Twitter have followed suit, and the use of HTTPS is expected to continue to grow in the future.

Figure 7 compares trends in TCP port usage over a week for overall traffic in 2013 and 2014. Trends in TCP port usage are shown for three categories: port 80, other well-known ports, and dynamic ports. Traffic is normalized by the total peak traffic volume. Compared with 2013, we can see that the overall ratio of port 80 usage has increased further, and the use of dynamic ports is decreasing. The overall peak is between 21:00 and 1:00, and traffic also increases in the daytime on Saturday and Sunday, reflecting times when the Internet is used at home.

In the same way, Figure 8 and Figure 9 compare weekly TCP port usage trends for client-type and peer-type users in 2013 and 2014. Most client-type user traffic is port 80, but the ratio of other well-known ports including the port for HTTPS is increasing. Peak times are between 21:00 and 23:00. Additionally, for peer-type users, the ratio of port 80 traffic exceeded the ratio for dynamic ports for the first time.

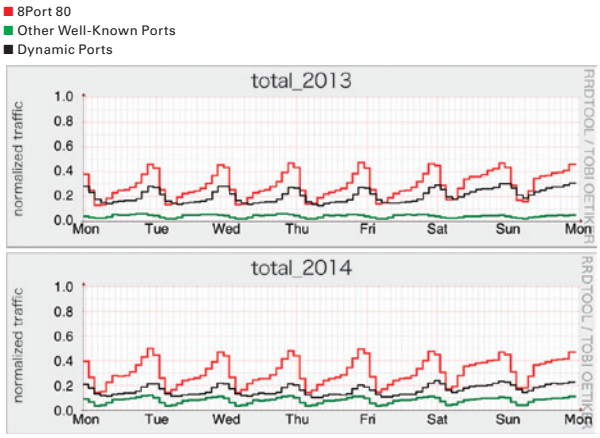


Figure 7: Weekly TCP Port Usage Trends 2013 (top) and 2014 (bottom)

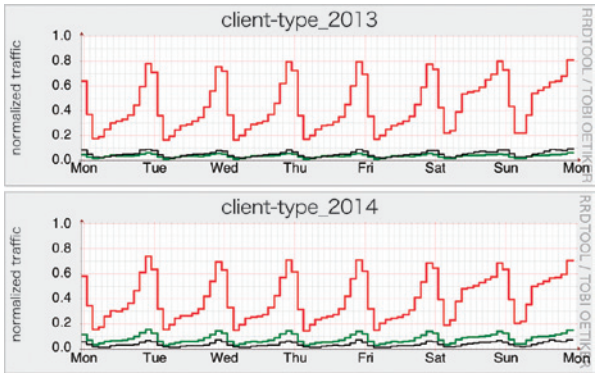


Figure 8: Weekly TCP Port Usage Trends for Client-Type Users 2013 (top) and 2014 (bottom)

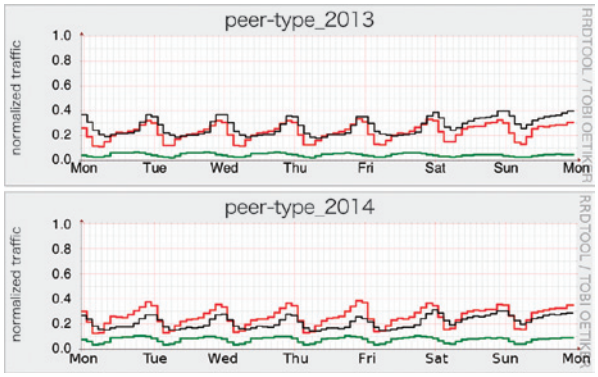


Figure 9: Weekly TCP Port Usage Trends for Peer-Type Users 2013 (top) and 2014 (bottom)

2.5 Conclusion

These results demonstrate that there were no large changes in the overall trends for broadband traffic over the past year. Traffic volumes are growing steadily, with overall download volumes up 27%, and uploads also increasing 13%.

For Web traffic, which now makes up the majority of traffic, we saw that the use of HTTPS is increasing. Google currently seems to be leading the pack in this regard, but other companies are also starting to make regular use of HTTPS in response to increased awareness of the importance of protecting privacy, and we expect the ratio of HTTPS traffic to continue to grow in the coming years.

In other news, NTT East finally launched its 1 Gbps broadband services in July 2014. NTT West has provided 1 Gbps services since 2010. As of now, the traffic for users of 1 Gbps services in Western Japan does not seem to differ significantly from other users, so there may not be many users that require a gigabit of bandwidth yet. However, the same was said when 100 Mbps fiber-optic access services began in 2001. I believe that broadband services are now facing a very important turning point, 13 years after fiber-optic access services were introduced.

Regarding protocols, HTTP/2 is currently in the planning phase, with major revisions expected to be made for the first time in 15 years. HTTP/2 will incorporate upgrades such as improved performance and more efficient use of network resources. As these kinds of generational shifts in infrastructure and protocols progress we will see a new environment emerge, paving the way for next-generation applications and services. That is why all eyes will be on the upcoming adoption of 1 Gbps services, and the resulting traffic increases and shifts in content. IIJ plans to continue to observe traffic on an ongoing basis, and provide periodic reports.

Author:

Kenjiro Cho
Research Director, Research Laboratory, IIJ Innovation Institute Inc.

The Environment Surrounding DNS

**DNS is used in many applications, serving as an important Internet service.
Here we discuss name collision issues that have arisen with recent TLD additions,
and examine the latest trends in the environment surrounding DNS.**

3.1 The Latest DNS Trends

DNS is a service that returns records in response to queries, and is mainly used for name resolution when looking up the IP addresses that correspond to domain names. Most applications on the Internet use name resolution via DNS, so it is a very important service. DNS involves authoritative servers for each zone that store records corresponding to domain names, and clients that make queries. In most cases, clients ask for DNS cache servers maintained by ISPs, etc., to perform laborious DNS recursive lookups, and only receive the results. DNS cache servers only know the IP address of the authoritative server that provides top-level zone information, which is known as the root. Based on the information gained from there, they track down authoritative servers likely to have more detailed information to locate the required record. Also, because server load and latency become an issue when making recursive queries each time, they cache the records obtained for a while, and retrieve records from the cache if the same query is received again. Recently, functions related to DNS have also begun to be implemented in devices on the communication route, such as broadband routers or firewalls. These may be involved in relaying DNS queries or applying control policies.

A governing organization known as a registry is specified and managed for each top-level domain (TLD), to prevent duplicate domain name spaces being registered. The root zone information is managed by ICANN, and from here authority is passed on to each TLD registry for the processing of domain name registrations from registrants. When registering a new domain name, an application is made to the TLD registry for the domain name you want to register through an intermediary called a registrar. However, each top-level domain and its associated subdomains have their own registration policies, and the details of who can register domain names for what purposes may vary. For example, .jp domains are governed by Japan Registry Services Co., Ltd. (JPRS), and any individual or company with an address in Japan that can be contacted is able to register the second-level domain names known as general-use jp. However, only companies and organizations registered in Japan can register domain names with a .co.jp suffix. Some TLDs are also run without any restrictions set, under a policy that allows anyone to register domain names. Because the management of registered domain names is delegated to the registrant, each registrant must have their own operation policy to manage and operate their domain appropriately.

3.2 Name Collision Issues

Systems introduced for the sake of convenience with the idea that some form of action is better than nothing can create problems down the line. Name collision issues are an example of this. For instance, in environments with clearly defined management that are only used by certain people, such as companies or homes, independent internal domain name spaces with a non-existent TLD (private TLD) may be used. For small scale operations, host names may be registered directly on clients using a hosts file, etc. When larger numbers of clients are involved, the DNS may be configured to respond to private TLD queries from an internal cache server or firewall, making access using an internal domain name possible without requiring any changes to client settings in particular. A system may appear to be working according to plan when configured, but the Internet is continually evolving, and cracks can start to appear when standard technology is used under non-standard configurations. Over 300 new TLD have already been added to the root zone in recent years, and that number continues to grow. If a private TLD configured internally for convenience conflicts with an added TLD, it results in issues such as no longer being able to use legitimately registered domain names, or unintentional connection to sites. This is called name collision issues (Figure 1). To avoid these issues it is important to preserve uniqueness for domain names, even if they are only for internal use. When you already have a domain name registered, you can be secure in the knowledge that the uniqueness of the domain name you use can be maintained in the future by configuring a subdomain for internal use under it, or preferably registering a new domain name for internal use.

Name collision issues also affect digital certificates for servers. Public certificate authorities that issue digital certificates have issued them even for private TLD domain names for internal use, so that digital certificates can also be used on the internal servers of organizations. Digital certificates for standard servers enable the ownership of domain names to be confirmed through the registration of specific character strings to email or websites. However, this kind of confirmation cannot be performed with private TLDs, so it was possible to obtain digital certificates without any confirmation in particular. As a result, when a domain name was registered to a newly added TLD, someone could have obtained a digital certificate for the corresponding domain name in the past. In response to these name collision issues, the CA/Browser Forum, a private organization involved with digital certificates, developed operational standards to gradually limit internal domain name digital certificates in the future. The digital certificates already issued for internal domain names are set to expire no later than November 1, 2015. When a new TLD is added, associated digital certificates are revoked within 120 days. There are also plans to revoke all digital certificates for internal domain names using a private TLD or domain names that cannot be confirmed to exist from the Internet, including those previously issued, in October 2016.

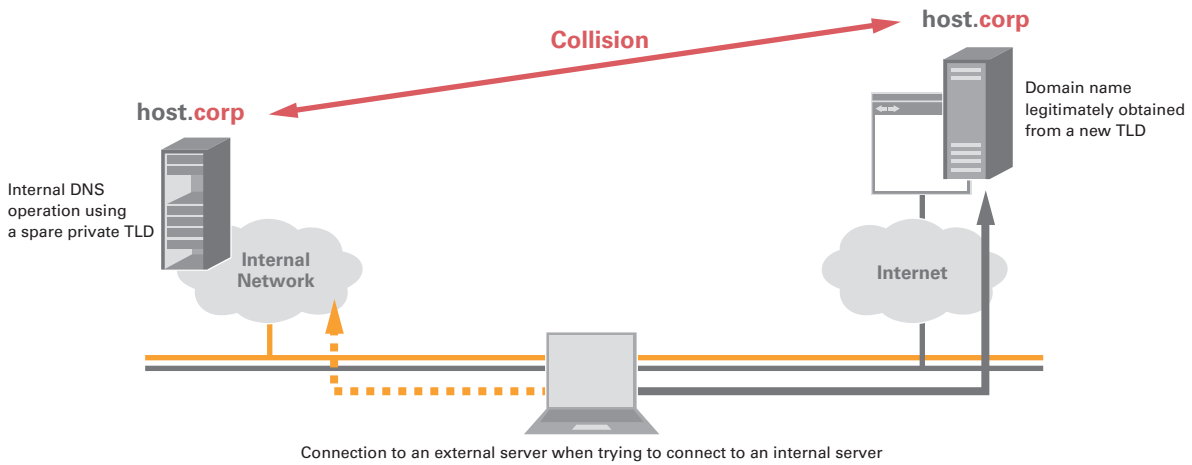


Figure 1: Name Collision Examples

Clients sometimes implement functions such as search lists and DNS suffixes for supplementing the domain name during DNS name resolution. These functions enable users to specify the intended domain name by entering the first part, rather than the fully qualified domain name (FQDN). Within organizations the domain name part is usually shared, so this function is used to enable connection to multiple servers or devices without having to repeatedly enter the same domain name. However, this is another area in which name collision issues crop up. Although largely dependent on the client implementation, when a domain name containing at least one "." is specified as the destination, it seems that in many cases the domain name is first queried via DNS, and then queried again with the addition of the search list domain name if no record exists. Consequently, when name resolution using the intended domain name was previously successful after the domain name was supplemented because a domain name corresponding to the initial query did not exist, there is a possibility of unintentionally connecting to the wrong site when a response to the initial query is obtained due to subsequent changes in the environment. Newly registered TLDs include regional names such as tokyo and nyc, so it is necessary to take particular care when using these regional names for subdomains. It goes without saying that thought must be given to the overall impact, considering all the TLD added, the operation of internal subdomains, and the DNS search lists distributed via DHCP, etc. To avoid trouble in the future, it would be best to instruct users to connect using fully qualified domain names whenever possible.

ICANN recognized the issues with name collision from an early stage, and they have taken a range of measures to lessen the impact. The CA/Browser Forum operational standards mentioned previously are the result of discussions with ICANN, and they have evaluated the risks associated with implementing new TLD based on actual DNS query status. Their investigation used data from major authoritative servers collected mainly during DNS-OARC's A Day in the Life of the Internet (DITL) project*1. Internal domain names are designed to be used within organizations, but DNS queries leak when there are configuration errors, or when mobile devices attempt to connect to servers from an external network. This can also be detected on root servers, allowing private TLD usage to be estimated. In this survey it was discovered that queries using "home" and "corp" private TLDs were remarkably frequent. Because there would be too many problems if these were recognized as new TLDs, it was decided that they should remain undelegated indefinitely*2. Other new TLDs can be delegated, with the caveat that registering certain second-level domain names that are highly likely to cause name collision is prohibited, based on their frequency of appearance in data such as DITL.

In Japan, JPNIC established a team of experts to evaluate risk and recommend strategies for the launch of a large number of gTLDs. They looked into name collision issues, and summarized their recommendations in writing*3. Because the impact of name collision issues can show up in unexpected places, I recommend a thorough review to check whether there are actually any dangers present. This should also cover areas that have functioned without issue before, including internal settings and URLs listed in documents.

*1 https://www.dns-oarc.net/oarc/data/ditl
*2 https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-1-07oct13-en.pdf
*3 https://www.nic.ad.jp/ja/dom/new-gtld/name-collision/

3.3 DNS and Communication Control

DNS has the capability to control and monitor the communications of users, such as redirection to websites and control of mail delivery. In other words, it is possible to control client communications by manipulating DNS responses (Figure 2). For example, providers that distribute content on a worldwide scale may have an implementation that responds to DNS queries from clients with the IP address of a delivery server close to the client, to reduce latency and optimize delivery. Because many users actually use the DNS cache servers provided by ISPs, etc., it seems the authoritative servers managed by content providers group users by DNS cache server, and respond with the IP address thought to be most suitable. Meanwhile, there have also been cases in which this has been exploited by attackers. Attackers often cause users to reference DNS cache servers they manage, resulting in the download of malicious content. In DNS Changer cases, it was reported that the DNS lookup address for a device was overwritten, and the DNS lookup address of broadband routers was changed to one controlled by the attacker. To avoid being redirected to malicious data like this, the utmost care must be taken with DNS settings, but the environment surrounding DNS is becoming more complicated.

Currently, most devices set the DNS cache server to look up based on DHCP information. In some cases the DHCP function is consciously activated by an administrator within an organization, while for consumer usage it may be provided as standard via a broadband router. Many broadband routers implement functions for simply relaying DNS queries to the DNS cache servers of ISPs, etc., and configure the router itself as the DNS lookup address for devices at home. However, with regard to DNS specifications, it seems these implementations sometimes only feature very limited functionality. They may lack support for queries over TCP, or not be fully compatible with EDNS0. In light of this situation, guidelines for implementing DNS relay functions in devices such as broadband routers were published as RFC5625/BCP152*4. These guidelines recommend that DNS relay functions be implemented with a focus on transparency, so they can continue to be used without issue in the future.

Some broadband router models forcibly send all DNS queries that pass through them on to the DNS cache server set on the router, regardless of the device's DNS lookup address settings. In this case, it is not possible to determine which DNS cache server is referenced simply by looking at the DNS lookup address settings on the device, no matter what IP address

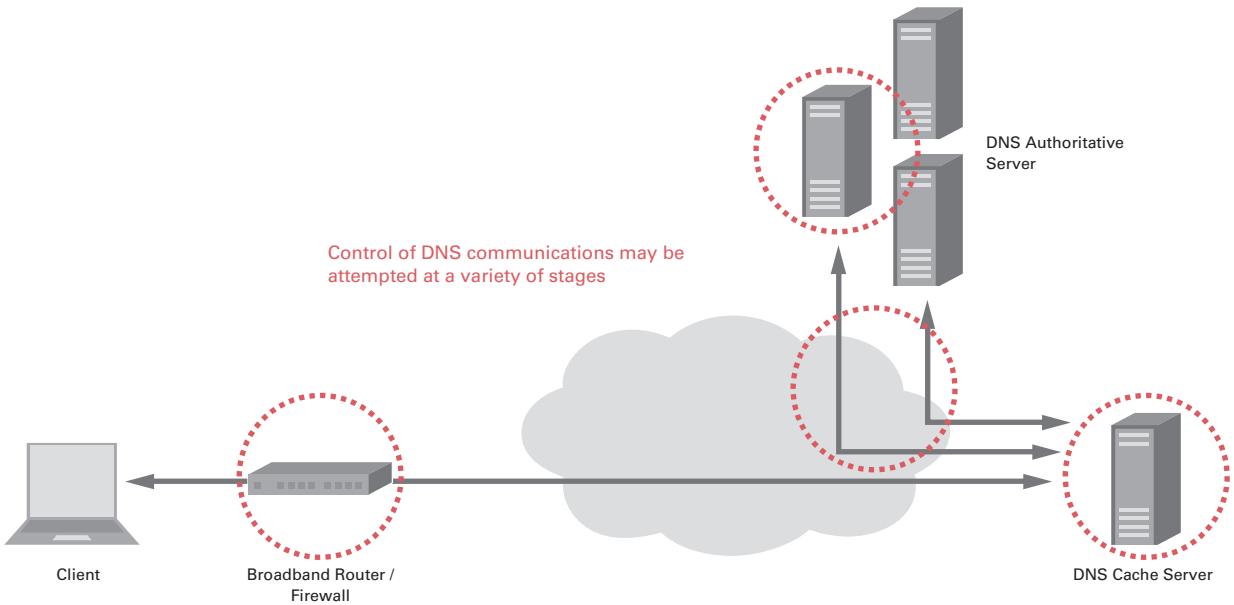


Figure 2: DNS and Communication Control

*4 https://tools.ietf.org/html/rfc5625

is registered to it. That is because as soon as a DNS query from the device passes over the broadband router, it is rewritten as a query to the specified DNS cache server. This may be a convenient function for implementing operation policies that enforce specific DNS cache servers, but it is harder for users to notice when a problem occurs, making isolation very difficult.

A variety of controls are also being implemented on ISP DNS cache servers. When devices connected to a walled garden IPv6 network communicate with servers on the Internet side via IPv4 alone, the IPv6 connection may fail, causing delays or connection faults due to IPv6/IPv4 fallback. Communication is also possible via IPv6 as long as an Internet connection exists, but because this requires an application and router update, there are concerns over the time it takes to implement. To alleviate problems in the user environment such as these, DNS cache servers may implement a function called an AAAA filter that gives no response for the AAAA records used with IPv6. Additionally, to prevent the circulation of child pornography, child pornography blocking*5 is sometimes implemented on DNS cache servers. This blocks responses for specific domain names.

In some countries and regions, DNS control has been introduced for the government-led blocking of access to undesirable content. Blocking is apparently carried out via the DNS cache servers provided by each ISP. Queries to specific domain names are also sometimes blocked, or the responses altered to contain falsified information, by implementing functions that monitor DNS queries on a network. Because users cannot determine whether issues are caused by communication faults or intentional blocking in most cases, and with blocking policies seldom being disclosed, it is tricky to figure out whether there is an issue and isolate the problem. However, as there are patterns in the content blocked depending on the country or region, it is possible to estimate whether intentional blocking is likely to be involved. This demonstrates that DNS control can be implemented in a variety of areas, and these must be considered when isolating an issue to pinpoint the obstruction.

3.4 DNS and Attacks

Because DNS is implemented on many devices, and many applications are practically reliant on it, it is sometimes exploited or targeted by attacks. DNS amplification attacks, which use DNS cache servers called open resolvers that respond to queries from anyone as stepping stones, have come to be particularly widely exploited due to their amplification efficiency and distributed nature. Many DNS cache servers were left to respond to queries from everyone without any countermeasures taken, so they were used as stepping stones. The configuration of DNS cache servers for ISPs in Japan has changed gradually in recent years, and they now usually only accept DNS queries from their users. However, some DNS relay functions implemented on broadband routers respond to DNS queries from the Internet without restriction by default, allowing them to be exploited as stepping stones in attacks. These must be dealt with individually by users, so continued reminders for users are required.

Attacks and the exploitation of DNS authoritative servers are also occurring. As with regular DDoS attacks, these aim to disrupt service by flooding authoritative servers with large volumes of traffic. There have also been cases in which authoritative servers have been exploited as stepping stones in DNS amplification attacks by directing large volumes of queries that are legitimate under DNS protocol at them. Straightforward traffic floods can be prevented through use of an appropriate packet filter. However when a server used as a stepping stone in an amplification attack, it is not easy to distinguish the queries intended as attacks, so the response must be considered. A number of authoritative DNS, including JP DNS, are making an effort to reduce the impact by implementing a function known as Response Rate Limiting (RRL), which limits a consecutive series of identical responses*6. However, this countermeasure is not foolproof, so it is necessary to continue scrutinizing attack techniques and searching for an appropriate response.

*5 http://www.netsafety.or.jp/blocking/
*6 http://www.redbarn.org/dns/ratelimits

Since the beginning of 2014, we have intermittently observed large volumes of DNS queries involving a number of domain names on ISP DNS cache servers. The purpose of these is not known, but our guess is that they are likely to be distributed attacks on the authoritative servers for the corresponding domain. However, because a large volume of communications with the corresponding authoritative servers is generated along with these attacks, even the DNS cache servers are overloaded, and at times faults such as delays involving name resolution for DNS cache server users occur. Regardless of whether or not this was the attacker's intention, when users are impacted some form of action must be taken. That said, because the communications appear identical to regular DNS queries from users, with broadband routers acting as open resolvers used as stepping stones in some cases, and DNS queries from bots that have infected user PCs used in others, it is not easy to apply generic countermeasures. We must pay close attention to the format of queries that appear with abnormal frequency, and take measures on a case-by-case basis.

UDP is usually used as the protocol for DNS queries. UDP communications are easier to spoof than TCP, and attackers may be able to inject fraudulent responses. For the injection of fraudulent responses to succeed, the query and IP address, port number, DNS ID, and QNAME information must match. To defend against this, it is necessary to ensure that information corresponding to queries does not match fraudulent responses. Assuming that the DNS ID is already generated from sufficiently random numbers, the only remaining option is to use a well-randomized number for the outgoing port number. When using old DNS implementations with a fixed outgoing port number, it will be necessary to upgrade to the latest DNS implementation to be able to send out queries that are hard to calculate. Also, because some firewalls and NAPT devices overwrite information such as the DNS ID and outgoing port number even when you've gone to the trouble of randomizing them, caution is required.

Spoofing of the source IP address is often used in attacks related to DNS. Once BCP38*7 is implemented on each network, creating environments in which the source IP address cannot be spoofed, it will be possible to eradicate most of the current attacks that exploit DNS. Routers are also equipped with a uRPF check function to make BCP38 easier to implement, so we recommend seriously considering the introduction of source IP address validation to prevent attacks in which the source IP address is spoofed, particularly in networks connected to devices.

3.5 Conclusion

DNS is a crucial Internet service that many applications depend on. To keep it available for use in a healthy condition, the authoritative servers, clients and DNS cache servers that carry out name resolution, and other equipment that interacts with DNS must be managed and operated with suitable coordination. DNS name spaces are changing significantly after the recent addition of new TLDs. When using domain names internally via private TLDs, or name resolution dependent on search lists, name collision issues may occur. Also, because DNS is widely used as a control system, and control attempts may be made in a variety of areas, it is becoming more complex. This complexity itself can be a source of problems, and could interfere with name resolution, so care must be taken. Although not limited to DNS, attack techniques are changing due to an abundance of bandwidth and CPU resources. We recommend a close eye be kept on attack techniques as they develop, as it will be necessary to gather and share information on a daily basis to keep up with the times. IIJ would like to contribute to the development of a healthy Internet by operating our facilities appropriately, and taking part in information sharing and discussion as needed.

Author:

Yoshinobu Matsuzaki
Mr. Matsuzaki is a Senior Engineer in the Network Engineering Section of IIJ Network Service Department.

*7 http://tools.ietf.org/html/bcp84

Vol.24 August 2014

About Internet Initiative Japan Inc. (IIJ)

IIJ was established in 1992, mainly by a group of engineers who had been involved in research and development activities related to the Internet, under the concept of promoting the widespread use of the Internet in Japan.

IIJ currently operates one of the largest Internet backbones in Japan, manages Internet infrastructures, and provides comprehensive high-quality system environments (including Internet access, systems integration, and outsourcing services, etc.) to high-end business users including the government and other public offices and financial institutions.

In addition, IIJ actively shares knowledge accumulated through service development and Internet backbone operation, and is making efforts to expand the Internet used as a social infrastructure.

Internet Initiative Japan Inc.
Address: Iidabashi Grand Bloom, 2-10-2 Fujimi, Chiyoda-ku, Tokyo 102-0071, Japan
Email: info@iij.ad.jp URL: http://www.iij.ad.jp/en/

IIJ-MKTG020VA-1410CP-00001PR