Internet Infrastructure Review

IIJ
Internet Initiative Japan

Vol.11

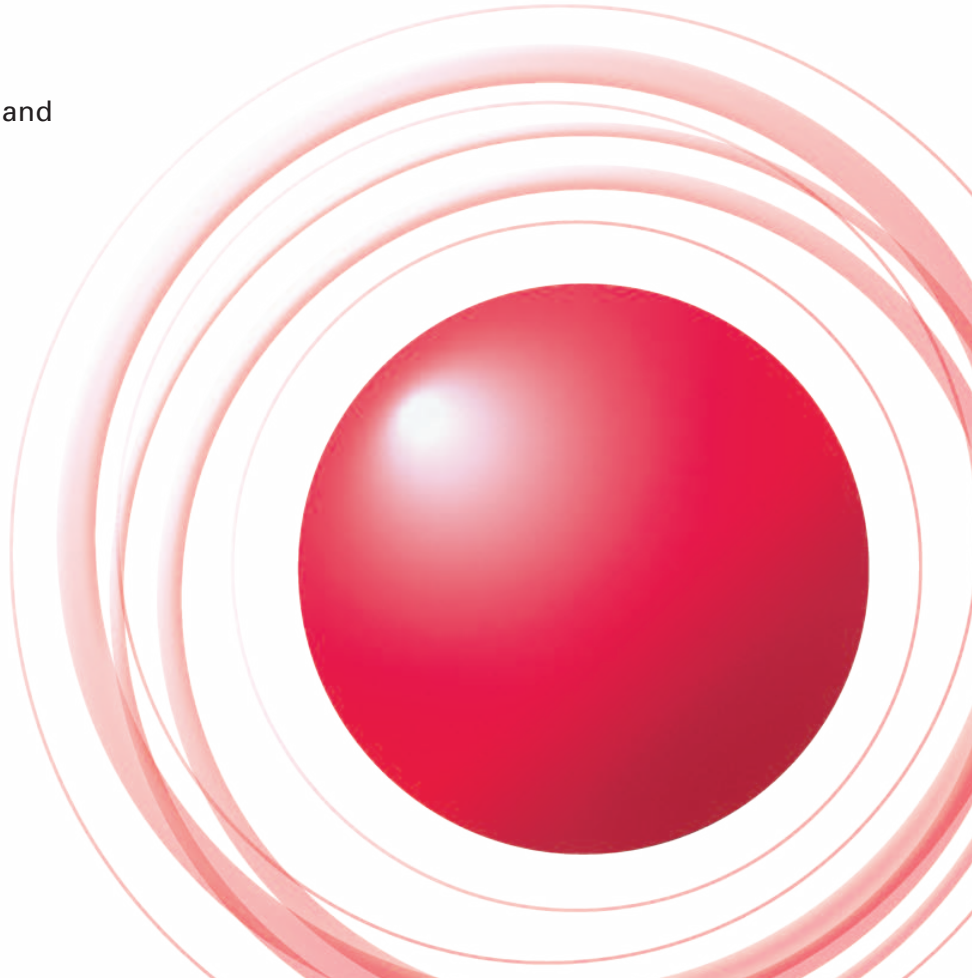
May
2011

Infrastructure Security
Security Incidents Related to the Great East Japan Earthquake

Messaging Technology
Why Japan Became the 3rd Largest Regional Source of Spam

Cloud Computing Technology
Web Access Consolidation and Access Pattern-Based Optimization for Web-based Service Platforms

Internet Operation
The IPv4 Address Exhaustion Issue and Guidelines for Response



Internet Infrastructure Review Vol.11 May 2011

■ To download the latest issue of the Internet Infrastructure Review, please visit (http://www.iij.ad.jp/en/development/iir/).

Executive Summary

The mission of Internet operation is to keep the Internet up and running all the time in order to secure the availability of smooth communications over this social infrastructure for anyone, anywhere and at any time. The Great East Japan Earthquake, however, caused extensive damage to various social infrastructures including the Internet in the East Japan region. We pray for the swift recovery of the devastated area, and we would like to pay sincere respects and express generous gratitude to the operators striving to restore the infrastructure necessary to achieve this.

Meanwhile, on April 15. 2011 the APNIC regional internet registry (IR) that Japan belongs to and the JPNIC IR in Japan ceased allocation of IPv4 addresses via their regular allocation policy and entered the final phase of allocation. This means that the free pool of IPv4 addresses at these registries is effectively exhausted.

The issue of IPv4 address exhaustion was first raised in 1992. Following this, design of new version of the Internet protocol to replace IPv4 began with the IETF playing a central role, and considerable research and preparation work has been carried out over the course of about 19 years. We are now finally approaching the stage where this research and preparation will be brought to fruition.

This report discusses the results of the various ongoing surveys and analysis activities that IIJ carries out to maintain and develop 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 report on the results of our ongoing statistics gathering and analyses for security incidents observed during the three months from January 1 to March 31, 2011. We also present our focused research for this period, discussing IIJ's new malware observation environment, the anti-forensic techniques employed by malware, and the impact of the Great East Japan Earthquake on telecommunications services in Japan, as well as related attacks.

In the "Messaging Technology" section, we examine spam ratio trends and regional source distribution, as well as trends in the main regional sources of spam, for 13 weeks between January and early April, 2011. We also discuss the relationship between botnet activity and regional sources of spam, analyze the connection between SPF authentication results and spam, and comment on the impact of IPv4 address exhaustion on anti-spam measures.

In the "Cloud Computing Technology" section, we discuss the results of our research into improving the utilization of large-scale Web servers, including simulation of the effect on overall traffic when Web content where access is concentrated is consolidated, and analysis of the variation in access frequencies over time for content where access is concentrated.

In the "Internet Operation" section, we examine the situation following the exhaustion of IPv4 addresses on April 15, 2011 and look at efforts towards improving the utilization of IPv4 addresses and migrating to IPv6 that will be necessary from now on, as well as issues related to these initiatives.

Under "Internet Topics," we provide an overview of the "World IPv6 Day" IPv6 trial event that was held around the world on June 8, 2011 to confirm the status of preparations for the migration to IPv6 and uncover outstanding issues, and also discuss initiatives within Japan.

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. 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 as executive vice president in charge of technical development in 2004. Mr. Asaba founded the IIJ Innovation Institute Inc. in June 2008, and became president and CEO of that organization.

Security Incidents Related to the Great East Japan Earthquake

In this report we will examine malware observation implementations and techniques used by malware to avoid forensic detection, in addition to discussing the state of communications in Japan following the Great East Japan Earthquake and related security incidents.

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 January 1 through March 31, 2011. In this period a number of vulnerabilities related to Web browsers and their plug-ins continued to be exploited, and incidents relating to mobile phones and cloud computing were also on the rise. There were also attacks relating to political turmoil in the Middle East, and DDoS attacks utilizing malware in South Korea. Additionally, the state of domestic communications was subject to change due to the Great East Japan Earthquake, and attacks taking advantage of the disaster occurred. As seen above, the Internet continues to experience many security-related incidents.

1.2 Incident Summary

Here, we discuss the IIJ handling and response to incidents that occurred between January 1 and March 31, 2011. Figure 1 shows the distribution of incidents handled during this period*1.

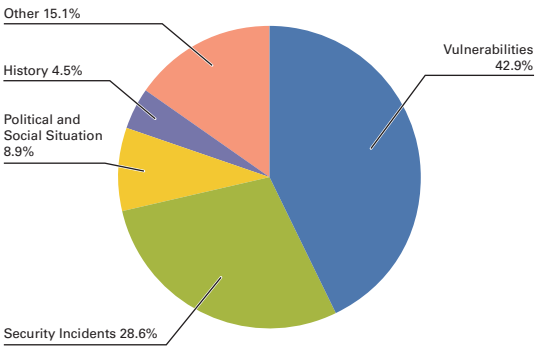


Figure 1: Incident Ratio by Category (January 1 to March 31, 2011)

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

Vulnerabilities

During this period a large number of vulnerabilities were discovered and fixed in Web browsers and applications such as Microsoft's Internet Explorer*2 and Windows*3*4*5, Adobe System's Adobe Reader and Acrobat*6*7, Flash Player*8*9, and Shockwave Player*10, and Oracle's JRE*11. Multiple vulnerabilities were also fixed in Apple's Mac OS X*12. Several of these vulnerabilities were exploited before patches were released.

Many vulnerabilities were also patched in server applications such as Microsoft's Internet Information Services (IIS) FTP service*13, the vsftpd FTP server*14 used in systems such as Linux, Oracle's Oracle Database*15 database server, the ISC BIND*16 DNS server, and the CMS platform WordPress*17. Additionally, vulnerabilities were discovered and fixed in Apple's iOS*18 platform for mobile phones.

Political and Social Situations

IIJ pays close attention to various political and social situations related to international affairs and current events. During this period Internet shutdowns*19 and large-scale DDoS attacks*20 occurring in connection with political turmoil in countries such as Tunisia and Egypt garnered considerable attention. However, IIJ did not detect any directly-connected attacks on IIJ facilities or our client networks.

History

The period in question included several historically significant days on which incidents such as DDoS attacks and website alterations have occurred. For this reason, close attention was paid to political and social situations. However, IIJ did not detect any direct attacks on IIJ facilities or our client networks.

Security Incidents

Unanticipated security incidents not related to political or social situations occurred, including the discovery overseas of a virus targeting the Android OS mobile phone platform*21, and reports of scareware that pretends to be legitimate

*2 Microsoft Security Bulletin MS11-003 - Critical: Cumulative Security Update for Internet Explorer (2482017) (http://www.microsoft.com/technet/security/bulletin/ms11-003.mspx).
*3 Microsoft Security Bulletin MS11-006 - Critical: Vulnerability in Windows Shell Graphics Processing Could Allow Remote Code Execution (2483185) (http://www.microsoft.com/technet/security/bulletin/ms11-006.mspx).
*4 Microsoft Security Advisory (2501696) Vulnerability in MHTML Could Allow Information Disclosure (http://www.microsoft.com/technet/security/advisory/2501696.mspx). This vulnerability was fixed in April through Microsoft Security Bulletin MS11-026 - Important: Vulnerability in MHTML Could Allow Information Disclosure (2503658) (http://www.microsoft.com/technet/security/bulletin/ms11-026.mspx).
*5 Microsoft Security Bulletin MS11-015 - Critical: Vulnerabilities in Windows Media Could Allow Remote Code Execution (2510030) (http://www.microsoft.com/technet/security/bulletin/ms11-015.mspx).
*6 APSB11-03 Security updates available for Adobe Reader and Acrobat (http://www.adobe.com/support/security/bulletins/apsb11-03.html).
*7 APSB11-06 Security updates available for Adobe Reader and Acrobat (http://www.adobe.com/support/security/bulletins/apsb11-06.html).
*8 APSB11-02 Security update available for Adobe Flash Player (http://www.adobe.com/support/security/bulletins/apsb11-02.html).
*9 APSB11-05 Security update available for Adobe Flash Player (http://www.adobe.com/support/security/bulletins/apsb11-05.html).
*10 APSB11-01 Security update available for Shockwave Player (http://www.adobe.com/support/security/bulletins/apsb11-01.html).
*11 JavaTM SE 6 Update Release Notes (http://www.oracle.com/technetwork/java/javase/6u24releasenotes-307697.html).
*12 About the security content of Mac OS X v10.6.7 and Security Update 2011-001 (http://support.apple.com/kb/HT4581).
*13 Microsoft Security Bulletin MS11-004 - Important: Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution (2489256) (http://www.microsoft.com/technet/security/bulletin/ms11-004.mspx).
*14 A vulnerability was found in vsftpd before 2.3.3. This information is managed as CVE-2011-0762 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0762).
*15 Oracle Critical Patch Update Advisory - January 2011 (http://www.oracle.com/technetwork/topics/security/cpujan2011-194091.html).
*16 BIND: Server Lockup Upon IXFR or DDNS Update Combined with High Query Rate (http://www.isc.org/software/bind/advisories/cve-2011-0414).
*17 WordPress 3.0.5 (and 3.1 Release Candidate 4) (http://wordpress.org/news/2011/02/wordpress-3-0-5/).
*18 About the security content of iOS 4.3 (http://support.apple.com/kb/HT4564).
*19 Details of this incident can be found in the following Arbor Networks' security blog post, "Egypt Loses the Internet" (http://asert.arbornetworks.com/2011/01/egypt-loses-the-internet/).
*20 Details of this incident can be found in the following Sophos Naked Security blog post. "Egypt versus the internet - Anonymous hackers launch DDoS attack" (http://nakedsecurity.sophos.com/2011/01/26/egypt-versus-the-internet-anonymous-hackers-launch-ddos-attack/).
*21 Information-technology Promotion Agency, Japan (IPA) "Security alert for a virus targeted at Android OS" (http://www.ipa.go.jp/security/topics/alert20110121.html) (in Japanese).

software using validly signed files*22. SSL certificates for some major sites were also issued without authorization*23, and an update released to revoke these certificates in Web browsers and prevent them from being exploited*24.

Attacks targeting vulnerabilities in specific servers such as the Exim MTA*25, and unauthorized communications with SIP servers*26 continue to be uncovered, and unauthorized use of publicly accessible servers using these vulnerabilities has taken place*27. In South Korea, attacks similar to the DDoS attacks that occurred in July 2009 resurfaced again on March 3*28. There have also been many attempted malware infections utilizing email and SNS*29, and attacks exploiting cloud environments*30.

■ Other

As for other incidents, we focused on trends for incidents related to natural disasters such as the earthquake that struck New Zealand in February and the Great East Japan Earthquake in March. We confirmed SEO poisoning attacks*31 and targeted attacks*32 that took advantage of these major disasters. Regarding security-related trends, in December a DS record of the JP zone was registered into the root zone, and in January DNSSEC was implemented for JP domain name services*33.

Additionally, unallocated IPv4 addresses managed by the IANA (Internet Assigned Numbers Authority) were all released, bringing IPv4 address exhaustion closer to becoming a reality*34. The IPA also issued a report titled "10 Major Security Threats for the Year 2011: Evolving Attacks - Are Your Countermeasures Adequate?" that summarized the security incidents that occurred in 2010*35, and five telecommunications industry associations issued guidelines to help telecommunications carriers identify high volume communications such as DDoS attacks and implement suitable countermeasures titled "Guidelines for Dealing with High Volume Communications and Privacy at Telecommunications Carriers"*36.

*22 Symantec Security Response Blog "Using Trusted Software to do the Dirty Work" (http://www.symantec.com/connect/blogs/using-trusted-software-do-dirty-work).

*23 Details can be found in the following F-Secure blog post. "Rogue SSL Certificates ('Case Comodogate')" (http://www.f-secure.com/weblog/archives/00002128.html).

*24 In this case, certificates for popular websites issued through unauthorized use of the systems of the affected certificate issuing institution were added to the certificate revocation list (CRL), but depending on Web browser implementation and settings there was a chance that fraudulent websites could be treated as legitimate, so a system for explicitly invalidating those individual certificates was distributed via a browser patch. For example, "Microsoft Security Advisory (2524375) Fraudulent Digital Certificates Could Allow Spoofing" (http://www.microsoft.com/technet/security/advisory/2524375.mspx), or Mozilla Firefox's "Firefox Blocking Fraudulent Certificates" (http://blog.mozilla.com/security/2011/03/22/firefox-blocking-fraudulent-certificates/).

*25 Details of this incident can be found in the following IBM Tokyo SOC Report. Tokyo SOC Report "Attacks Attempting to Infect Servers with Bots Exploiting an Exim Vulnerability" (https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/exim_attack_20110309?lang=en_us) (in Japanese).

*26 cNotes provides SIP observation data on an irregular basis. For example, a list of IP addresses of attackers classified by country from 2011. "Fraudulent Incoming SIP 42 - From 2011 Forward" (http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=%C9%D4%C0%B5%A4%CASIP%C3%E5%BF%AE+42+2011%C7%AF%A4%CB%C6%FE%A4%C3%A4%C6) (in Japanese).

*27 JPCERT Coordination Center (JPCERT/CC) "Security settings of Internet servers (mainly UNIX / Linux servers)" (http://www.jpcert.or.jp/english/at/2011/at110002.txt).

*28 "AhnLab Issues Alerts Concerning DDoS Attacks on 40 Websites in South Korea" (http://www.ahnlab.co.jp/company/press/news_release_view.asp?se%20archWord=&movePage=&seq=5568) (in Japanese).

*29 Details can be found in the following Trend Micro security blog post. "Malicious Programs with File Names including Earthquake, Tsunami, Nuclear Power Stations, and Power Conservation Spread in Japan" (http://blog.trendmicro.co.jp/archives/4001) (in Japanese).

*30 A detailed report on attacks from cloud environments in 2010 is given in the following IBM Tokyo SOC Report. Tokyo SOC Report "Attacks Exploiting the Cloud" (https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/cloud-attack_20110216?lang=en_us) (in Japanese).

*31 Details can be found in the following Trend Micro malware blog post. "3/11 Japan Earthquake Disaster Scam Watch" (http://blog.trendmicro.com/most-recent-earthquake-in-japan-searches-lead-to-fakea/).

*32 For example, the following monthly report from Trend Micro. "March 2011 Monthly Report on Internet Threats: Cyber Attacks Taking Advantage of Earthquake - Beware of Techniques Capitalizing on Human Psychology" (http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20110406083423.html) (in Japanese).

*33 Japan Registry Services (JPRS) "JPRS Deploys DNSSEC in the JP Domain Name Service" (http://jprs.co.jp/en/press/2011/110117.html).

*34 Japan Network Information Center (JPNIC) "IANA's free pool of IPv4 address space depleted, and JPNIC's action hereafter" (http://www.nic.ad.jp/ja/topics/2011/20110204-01.html) (in Japanese).

*35 Information-technology Promotion Agency, Japan (IPA) "10 Major Security Threats for the Year 2011: Evolving Attacks - Are Your Countermeasures Adequate?" (http://www.ipa.go.jp/about/press/20110324.html) (in Japanese).

*36 The Council for Stable Operation of the Internet is comprised of five industry associations with links to the telecommunications business. Refer to the website below for details on the establishment of these guidelines. Japan Internet Provider's Association (JAIPA) "Revision to Guidelines for Dealing with High Volume Communications and Privacy at Telecommunications Carriers" (http://www.jaipa.or.jp/other/mtcs/info_110325.html) (in Japanese).

1.3 Incident Survey

Of incidents occurring on the Internet, IIJ focuses on those types of incidents that have infrastructure-wide effects, continually conducting research and engaging in countermeasures. In this section, we provide a summary of our survey and analysis results related to the circumstances of DDoS attacks, malware infections over networks, and SQL injections on Web servers.

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 utilize 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 January 1 and March 31, 2011. This information shows the number of traffic anomalies judged to be attacks based on IIJ DDoS Defense Service standards. IIJ also responds to other 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*37, attacks on servers*38, 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 585 DDoS attacks. This averages to 6.5 attacks per day, indicating an increase in the average daily number of attacks compared to our prior report. Bandwidth capacity attacks accounted for 0% of all incidents, server attacks accounted for 76% of all incidents, and compound attacks accounted for the remaining 24%.

The largest attack observed during the period under study was classified as a compound attack, and resulted in 163Mbps of bandwidth using up to 57,000pps packets. Of all attacks, 85% ended within 30 minutes of commencement, and 15% lasted between 30 minutes and 24 hours. No attacks continued for longer than 24 hours. The longest sustained attack during the current period was a server attack that lasted for six hours. In most cases, we observed

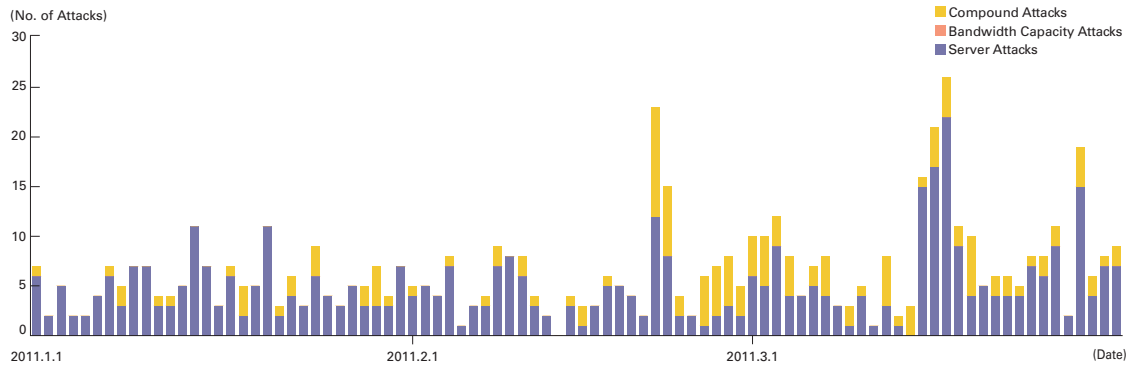


Figure 2: Trends in DDoS Attacks

*37 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.

*38 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.

an extremely large number of IP addresses, whether domestic or foreign. We believe this is accounted for by the use of IP spoofing*39 and botnet*40 usage as the method for conducting DDoS attacks.

Backscatter Observations

Next we present our observations of DDoS backscatter using the honeypots*41 set up by the MITF, a malware activity observation project operated by IIJ*42. By monitoring backscatter it is possible to detect DDoS attacks occurring on external networks as a third party without any interposition. For the backscatter observed between January 1 and March 31, 2011, Figure 3 shows trends in packet numbers by port, and Figure 4 shows the sender's IP addresses classified by country.

The port most commonly targeted by the DDoS attacks observed was the 80/TCP port used for Web services, accounting for 34.0% of the total during the target period. Attacks on 3389/TCP used for remote desktop were also observed. Looking at the origin of backscatter thought to indicate IP addresses targeted by DDoS attacks by country in Figure 4, the United States, Argentina, and China accounted for large proportions at 26.4%, 21.4% and 21.3%, respectively, with other countries following in order.

From the second half of February we observed an increase in the number of attacks classified under other categories, but most were attacks targeted at a wide range of ports for multiple addresses in Argentina. Ports were attacked in ascending order for certain addresses, with communications appearing similar to a port scan, but because the attacker cannot receive responses due to IP spoofing the reason for this behavior is unclear.

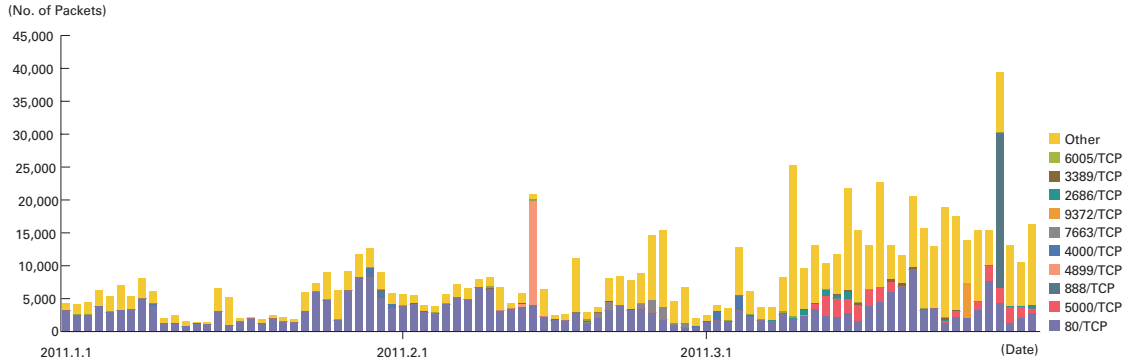


Figure 3: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)

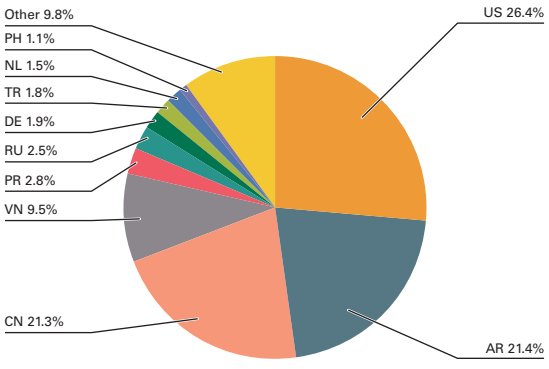


Figure 4: Distribution of DDoS Attack Targets According to Backscatter Observations (by Country, Entire Period under Study)

*39 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 in order to pretend that the attack is coming from a different location, or from a large number of individuals.

*40 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."

*41 See also "1.3.2 Malware Activities."

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

During the current period under study there were DDoS attacks on Middle-Eastern countries such as Egypt (second half of January), attacks on wordpress.com (early March), and DDoS attacks in South Korea (March 4), and we detected attacks on two sites in Egypt over the course of our observations. We believe that other attacks either did not involve IP spoofing, or used addresses other than those for IIJ observational equipment.

1.3.2 Malware Activities

Here, we present the results of the observations of the MITF*43, IIJ's malware activity observation project. The MITF uses honeypots*44 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 from malware selecting a target at random, or scanning behavior attempting to locate a target to attack.

■ Status of Random Communications

Figure 5 shows trends in the total volumes of communications coming into the honeypots (incoming packets) between January 1 and March 31, 2011. Figure 6 shows the distribution of sender's IP addresses by country. 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.

Much of the communications arriving at the honeypots demonstrated scanning behavior targeting TCP ports utilized by Microsoft operating systems. We also observed scanning behavior for 1433/TCP used by Microsoft's SQL Server and 80/TCP used for HTTP. Additionally, communications of an unknown purpose were observed on ports not used by common applications, such as 2582/TCP, 9230/UDP, and 28002/TCP. Looking at the overall sender distribution by country in Figure 6, we see that attacks sourced to Japan at 31.9% and China at 9.8% were comparatively higher than the rest.

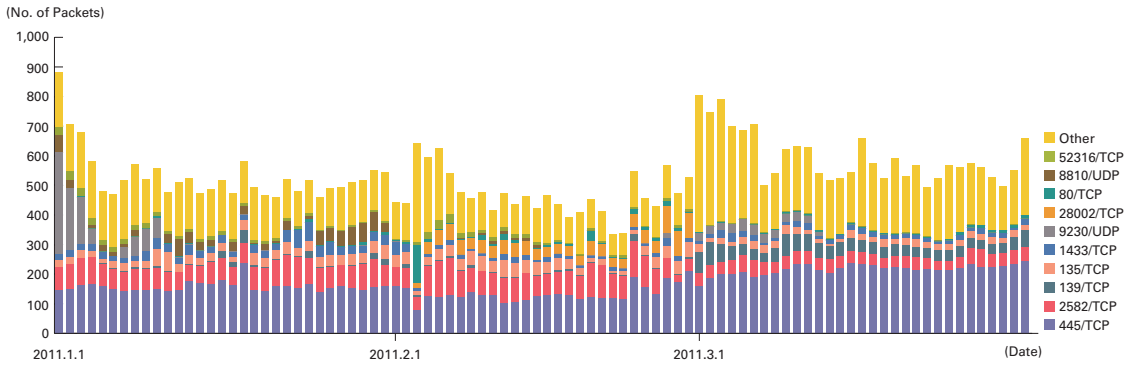


Figure 5: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

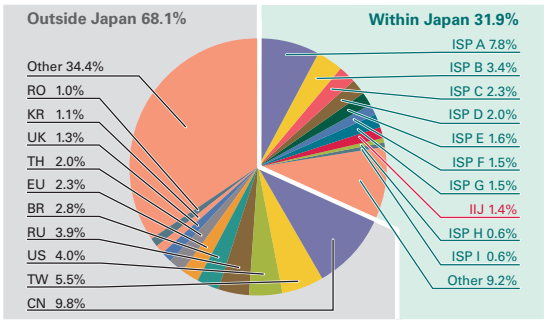


Figure 6: Sender Distribution (by Country, Entire Period under Study)

*43 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.

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

Malware Network Activity

Figure 7 shows trends in the total number of malware specimens acquired during the period under study. Figure 8 shows the distribution of the specimen acquisition source for malware. In Figure 7, the number of acquired specimens show the total number of malware specimens acquired by the honeypots per day, while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*45.

On average, 307 specimens were acquired per day during the period under study, representing 37 different malware variants. According to the statistics in our prior report, the average daily total for acquired specimens was 190, with 30 different variants.

The distribution of specimens according to source country in Figure 8 had Japan at 10.5%, with other countries accounting for the 89.5% balance. Taiwan was at 28.8%, maintaining the large ratio that it held during the previous period. This was due to the heightened activity of Mybot and its variants during this period, which was particularly predominant in Taiwan.

The MITF prepares analytical environments for malware, conducting its own independent analyses of acquired specimens. During the current period under observation 48.7% of the malware specimens acquired were worms, 44.3% were bots, and 7.0% were downloaders. In addition, the MITF confirmed through the analyses the presence of 48 botnet C&C servers*46 and 59 malware distribution sites.

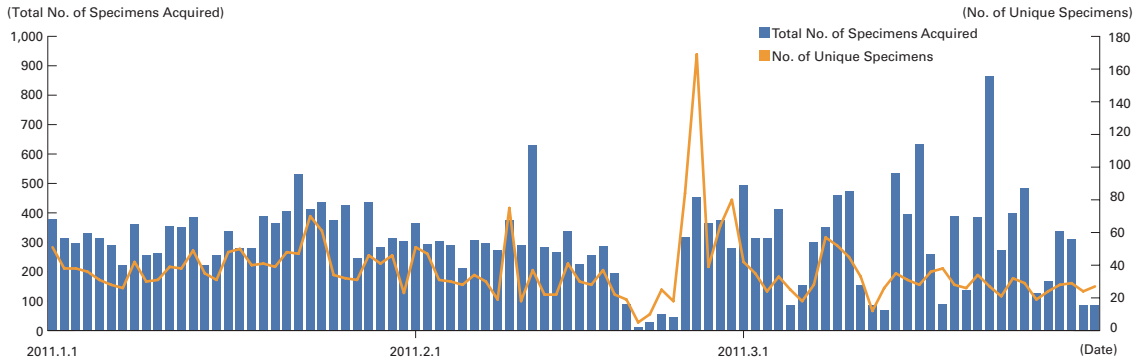


Figure 7: Trends in the Number of Malware Specimens Acquired (Total Number, Number of Unique Specimens)

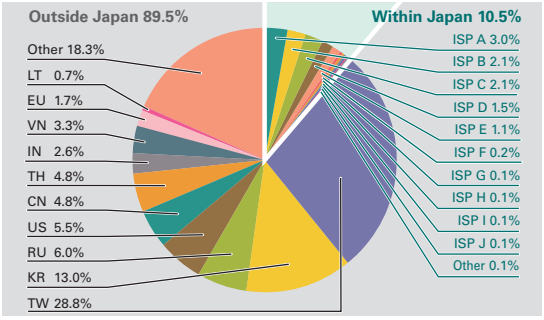


Figure 8: Distribution of Acquired Specimens by Source (by Country, Entire Period under Study)

*45 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.

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

1.3.3 SQL Injection Attacks

Of the types of different Web server attacks, IIJ conducts ongoing surveys related to SQL injection attacks*47. 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 9 shows trends in the numbers of SQL injection attacks against Web servers detected between January 1 and March 31, 2011. Figure 10 shows the distribution of attacks according to source. These are a summary of attacks detected by signatures on the IIJ Managed IPS Service.

Japan was the source for 48.2% of attacks observed, while the United States and China accounted for 21.2% and 5.1%, respectively, with other countries following in order. There was very little change from the previous period in the number of SQL injection attacks against Web servers that occurred. However, there were some focused attacks on a number of servers, such as a large-scale attack from the United States on a specific server on January 29, and attacks originating from both Japan and foreign sources on other servers on March 2, March 8, and March 22. They led to an increase in the overall ratios for Japan and the United States, and lowered the ratio of attacks from countries such as China and South Korea. The LizaMoon*48 attack that involved website alterations using SQL injections also drew attention during this period, with small-scale attack attempts made on multiple servers between February 4 and mid-February.

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.

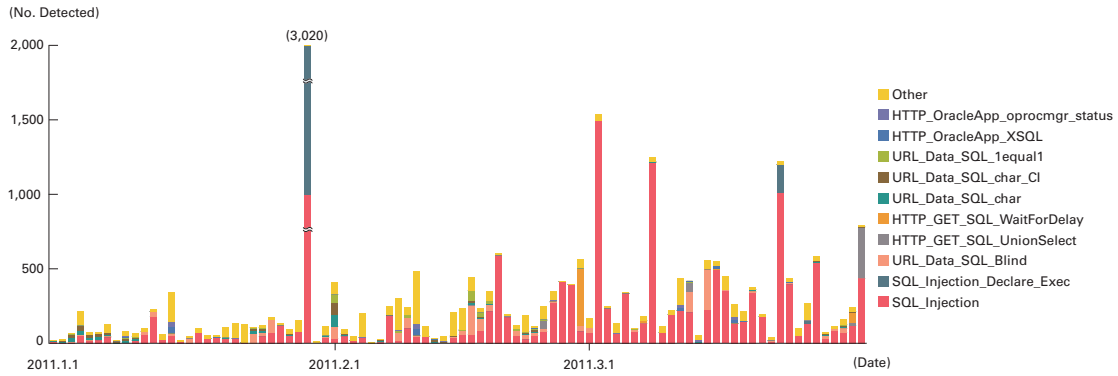


Figure 9: Trends in SQL Injection Attacks (by Day, by Attack Type)

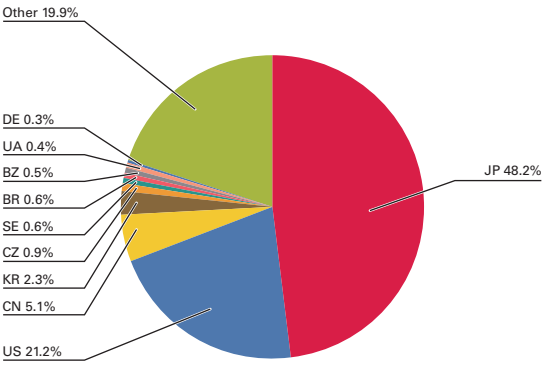


Figure 10: Distribution of SQL Injection Attacks by Source (by Country, Entire Period under Study)

*47 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.

*48 Details of the LizaMoon attack can be found in the following IBM Tokyo SOC Report. Tokyo SOC Report "A New Type of Website Alteration SQL Injection Attack" (https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/sqlinjection_20110401?lang=en_us) (in Japanese). Brief information in English is also available in the following blog article of IBM Internet Security Systems. Frequency X Blog "Analyzing a Mass SQL Injection Attack - Lizamoon" (http://blogs.iss.net/archive/lizamoon.html).

1.4 Focused Research

Incidents occurring over the Internet change in type and scope almost from one minute to the next. Accordingly, IIJ works toward taking countermeasures by continuing to perform independent surveys and analyses of prevalent incidents. Here we will discuss the newly-adopted Dionaea honeypot as well as malware anti-forensics, in addition to detailing Japan's communication circumstances after the Great East Japan Earthquake and attacks related to the disaster.

1.4.1 The Dionaea Honeypot

IIJ has carried out its MITF (Malware Investigation Task Force) anti-malware activities since May 2007*49. As part of these activities a honeypot*50 system was constructed to directly observe the activity of worms and bots attacking IIJ's network. Until now Nepenthes*51 was used for these observations. Here we discuss the functions and characteristics of the new Dionaea*52 honeypot system that we have put into operation.

■ Characteristics of Dionaea

Dionaea is honeypot software still under active development that was released in late May 2009 as a successor to Nepenthes. Dionaea features improvements over Nepenthes in areas such as malware acquisition and logging. Other characteristics of Dionaea include support for IPv6 and a python-based implementation that makes expansion easy. Here we will provide an overview of the following characteristics of Dionaea.

- Malware acquisition
- Improved attack detection accuracy
- Improved logging

One improvement to malware acquisition is support for new vulnerabilities. Nepenthes was only able to emulate vulnerabilities up to MS05-017. In contrast, Dionaea discontinues support for older vulnerabilities no longer commonly used in attacks, and has switched to a detection method that supports new vulnerabilities such as MS08-067*53.

Nepenthes used pattern matching on attack communications payloads to detect attacks. This led to the drawback of emulation being difficult when attacks were made after interaction using complex protocols such as SMB. Dionaea resolves this issue by implementing SMB and MSRPC protocol emulation. Additionally, by automatically detecting shellcode within a payload in conjunction with the Libemu*54 x86 emulator, it is possible to detect the exploitation of unknown vulnerabilities.

*49 MITF is explained in IIR Vol.7 under "1.4.3 MITF Anti-Malware Activities" (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol07_EN.pdf).
*50 Honeypots are systems for observing the techniques used by attackers, and include low-interaction types that emulate software with vulnerabilities and vulnerable systems, and high-interactions types that make use of actual OS and software implementations.
*51 Nepenthes (http://nepenthes.carnivore.it/) is a low-interaction server-based honeypot that mainly emulates known vulnerabilities in Microsoft's Windows. Its development has now been discontinued, and use of its successor Dionaea is recommended.
*52 Dionaea (http://dionaea.carnivore.it/).
*53 Microsoft Security Bulletin MS08-067 - Critical: Vulnerability in Server Service Could Allow Remote Code Execution (958644) (http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx).
*54 Libemu (http://libemu.carnivore.it/).

Next we will take a look at log-related functions. Dionaea can output logs in database format using SQLite in addition to logs in text format, making it easier to parse trends and analysis outputs. Nepenthes was only able to output time series logs, making it difficult to associate data at a later date. Meanwhile, Dionaea makes it possible to associate which attacks were included in which communications, and which communications led to malware being obtained.

A number of other improvements have also been made. Nepenthes only supported C++ for the addition of functions, but Dionaea makes it possible to write modules using Python, making it easier to expand functionality. Many other improvements not mentioned here were also made, such as support for IPv6.

■ Evaluation and Adoption of Dionaea

Dionaea was initially unstable, making everyday use difficult. Because its source code was updated on a daily basis*55, IIJ evaluated and tested Dionaea over time in tandem with Nepenthes. In these experimental observations we learned that the Conficker*56 malware that spreads via networks was extremely active. However, partly because there were few infections on the IIJ network, we gave priority to observation environment stability and continued observations using Nepenthes despite the fact that it could not obtain this malware, while also proceeding with our appraisal of Dionaea to adopt it at the MITF. While evaluating Dionaea we also considered other honeypot implementations*57. After comprehensive assessment of factors such as honeypot capabilities, community activeness, and compatibility with existing systems, we decided to construct a honeypot system based on Dionaea.

We began formal operation of this new observation system from March 2011. IIJ expanded upon the implementation of the new system to resolve functional inadequacies that were identified during evaluation, such as the inability to associate attacks and acquired malware, and the ambiguity of MSRPC commands included in attack code. We also revised the source code in order to apply it to IIJ's observation system environment. As previously mentioned, because it is now possible to emulate complex protocols, we can now observe attacks that involve multiple sets of communications. Because observations of connections to specific ports have increased as a result of this, we corrected the values observed for March to remove this influence from the figures in "1.3.2 Malware Activates." Additionally, because it was established that some malware such as Conficker performs repeated attacks on specific honeypots, we revised the system affected by this issue.

*55 The following URL lists the revision history of Dionaea (http://src.carnivore.it/dionaea/log/). As can be seen here, the source code was updated almost every day between late May 2009 when Dionaea was first committed and the second half of 2010, demonstrating how active its development was.

*56 See IIR Vol.2 under "1.4.2 Malware that Exploits MS08-067" (http://www.iij.ad.jp/development/iir/pdf/iir_vol02.pdf) (in Japanese) and IIR Vol.4 under "1.4.1 Worldwide Outbreak of the Conficker Malware" (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol04_EN.pdf) for more information on Conficker.

*57 For example, BotHunter (http://www.bothunter.net/), Amun (http://amunhoney.sourceforge.net/), and Argos (http://www.few.vu.nl/argos/).

■ Observations Using the New System

Figure 11 shows daily distribution and Figure 12 shows results by malware type for total specimens acquired in observation results using the new system. Malware names were identified using ClamAV and summarized in these figures. Comparing Figure 11 to the period up to February in Figure 7, we can see that acquisition status has changed significantly. The average total specimens acquired per day increased substantially from 307 under the old system to 25,246. This is due to the difference between Nepenthes and Dionaea in the number and types of vulnerability that can be emulated. The major difference between the two is that the new system makes it possible to obtain Conficker specimens.

Conficker is a worm that exploits the MS08-067 vulnerability to spread. Conficker (Worm.Kido and Worm.Downadup in the figure) accounts for a significant ratio of 71.4% of the total specimens acquired under the new system. Investigating the source of infection, 3.7% of sources were within Japan, with 0.03% from the IIJ network, showing that while it is not a major threat on the IIJ network, it remains very active on a global scale.

Thanks to this system change it is now easier to identify which malware is exploiting which vulnerability, enabling countermeasures to be implemented more swiftly. We can now also identify trends in malware that we could not obtain using Nepenthes. We are currently adjusting the system further with the aim of publishing data in this IIR on a regular basis. IIJ will continue to update our system in response to changes in circumstance and take appropriate measures to implement anti-malware activities.

1.4.2 Malware Anti-Forensics

When incidents such as unauthorized access or malware infections occur, digital forensic techniques*58 are used to investigate and analyze digital data on related devices. However, in recent years malware has begun to implement techniques called anti-forensics that hinder detection via analysis. Anti-forensics is carried out by deleting or changing

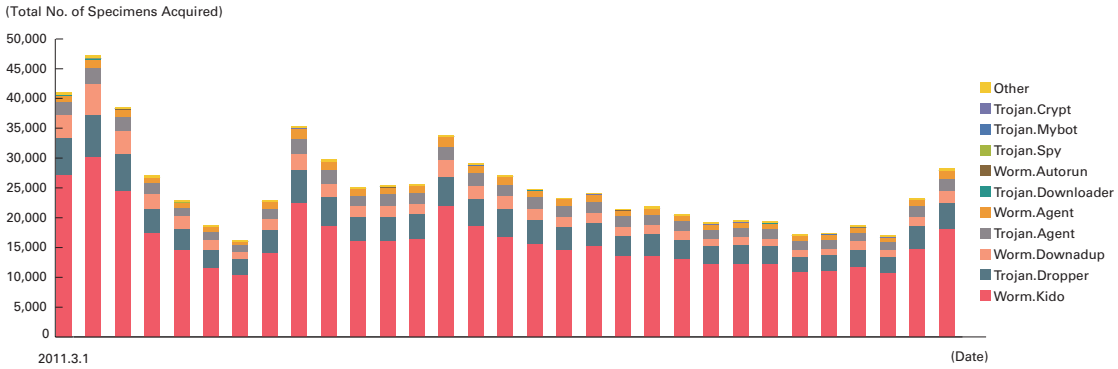


Figure 11: Trends in the Number of Malware Specimens Acquired (by Day, New System, by Specimen Type)

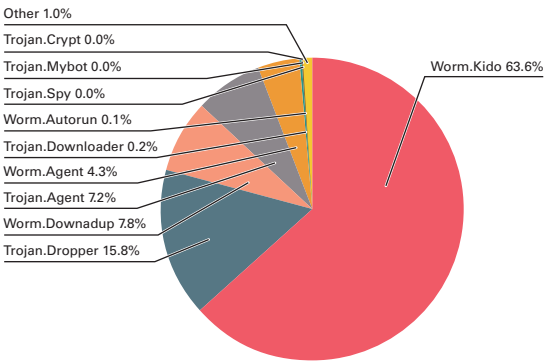


Figure 12: Distribution of Malware Specimens Acquired (March, by Specimen Type)

*58 See IIR Vol.9 under "1.4.3 An Overview of Digital Forensics" (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol09.pdf) for more information about digital forensic techniques.

the data found on media such as disks or memory. Here we introduce anti-forensic techniques that target the disks most commonly examined using forensic analysis (Windows file system), and discuss the measures that should be taken from an analyst's perspective.

■ Deletion of Files

The anti-forensic technique seen most often involves simply deleting files related to malware activity. When files are deleted they can no longer be seen from commonly-used software such as Windows Explorer. However, data is not erased immediately after a file is deleted. In fact, only part of the metadata for the corresponding file managed by the file system is changed*59. This means that it is possible to examine deleted files with software used in forensic analysis*60. In other words, it is possible to deal with concealment through this technique even when a file has been deleted as long as it has not been overwritten with another file.

■ Changes to Time Stamps

Another common technique involves changing the time stamp metadata of files. Computer hard disk drive capacities continue to increase in size every year, and can contain a large amount of data. For this reason analysis is sometimes narrowed down to the period that an incident occurred to limit the number of files for examination to as few as possible. Time stamp information such as the creation time and modification time of a file is used to filter files for a given period. Malware attempts to evade analysis by setting the time stamp information in files it wants to conceal to a completely different time using the SetFileTime API, etc. This technique began to be used in many malware such as Conficker about three years ago.

There are two methods of dealing with this technique. One method is to investigate the time stamps associated with data other than the target files. For example, Windows registry keys contain information about the time they were last modified. This means that target files can be detected for malware registered as a service by also checking the times in the registry. Additionally, Windows uses files to speed up execution called Windows Prefetch files that are generated each time an .exe file is executed. It is possible to pinpoint the time an .exe file was executed by checking the time stamp information in these prefetch files.

Another method of dealing with this is to use minor time stamp information that is not usually referenced to filter the period of time. Windows NTFS file systems store metadata including file time stamps in a special file called the MFT (Master File Table). File metadata is managed as entry attributes in the MFT. The time stamp information normally referenced is found in a Standard Information attribute, and this can be changed easily using API such as SetFileTime. Meanwhile, time stamp information for the File Name attribute cannot be changed via API. This means it is possible to invalidate time stamp changes carried out by malware by using time stamp information from the File Name attribute for filtering.

■ Deletion by Overwriting

Simple file deletion only changes part of the metadata, so the data in the file itself is not deleted. For this reason some malware uses the technique of deleting the very data in a file by overwriting it with random data. At IIJ we confirmed that the malware used to carry out widespread DDoS attacks in South Korea in early March this year employed this technique*61. It is difficult to identify the nature of malware when the data itself is overwritten, because it is not possible to analyze the malware dynamically or statically after this has taken place. However, because the metadata remains, it is possible to investigate related activities based on this. Additionally, although the chance of success is not very high, deleted files may be recoverable through automated backups using system restore functions (such as a Windows System Restore Point), so it is worth the check.

*59 When a file is deleted, the Windows NTFS file system only clears the flags that indicate the corresponding metadata and the disk space where the data is stored are in use. This means that as long as this disk space is not overwritten with another file, both the metadata and the file content remain.

*60 Examples of the software used for analysis include EnCase (http://www.guidancesoftware.com/), FTK (http://accessdata.com/), and TSK (http://www.sleuthkit.org/sleuthkit/).

*61 This malware was downloaded via file sharing sites, after which it launched a DDoS attack on specific sites and also destroyed the hard disk of the infected PC. Details of the behavior of this malware can be found in the following McAfee Blog post. McAfee Blog: "Malware in Recent Korean DDoS Attacks Destroys Systems" (http://blogs.mcafee.com/mcafee-labs/malware-in-recent-korean-ddos-attacks-destroys-systems).

Direct Access to File System

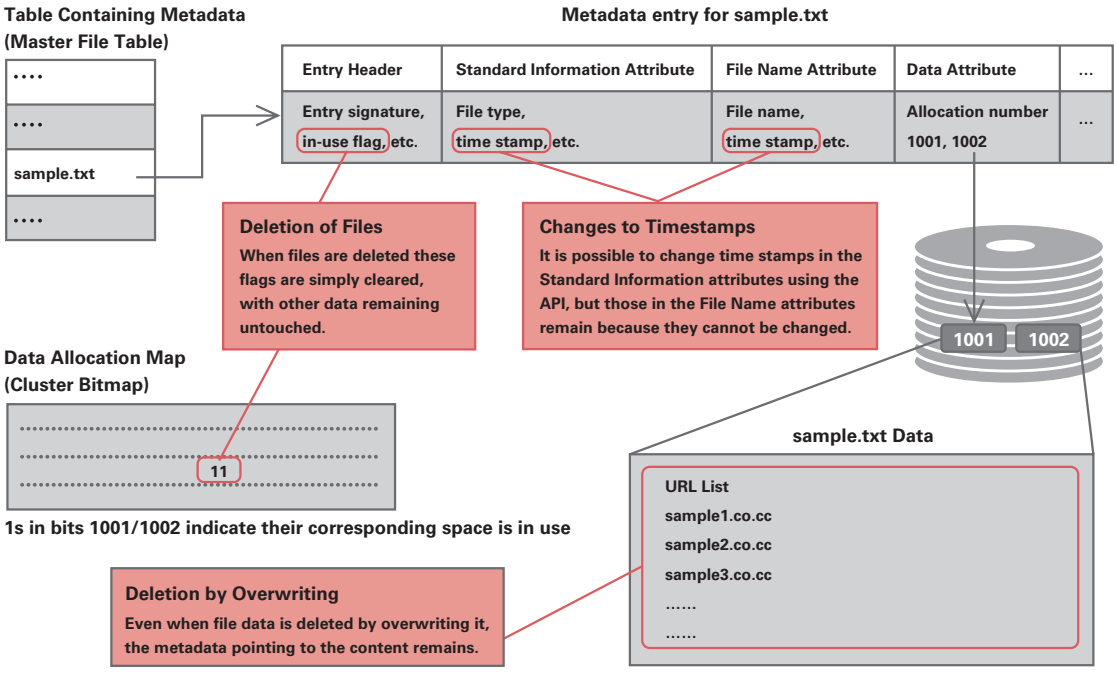
The anti-forensic techniques presented here all use system API to delete or change files. The data changed through these techniques is shown in Figure 13. As can be seen from this, regardless of which technique is used some traces are left in the file system metadata, and from this metadata it is possible to detect the affected files and investigate related activities.

However, recently malware that infects PC by analyzing the file system structure without using APIs has begun to appear. Backdoor.Prioxer*62, which Symantec reported on in March of this year, opens hard disk drives in RAW mode and identifies the type of file system used before locating files to infect in accordance with the algorithm for that file system and writing malicious code.

Investigation methods using metadata are not effective for this technique, making analysis that focuses on data content necessary. One example of this is comparing the hash values of file data. Because the files targeted for infection include many executables that are system standard, if hash values are calculated in advance for these executables in their normal state*63, it may be possible to detect infected files by comparing these hash values with those for the executables on an infected machine. IIJ has not observed any malware that uses this technique, but we are concerned that malware implementing such a technique may appear in the future.

Summary

Here we have presented a number of anti-forensic techniques used by malware. By implementing comprehensive analysis and avoiding one-sided analysis relying only on metadata or file content, analysts can deal with these to a certain extent no matter which technique is used*64. Here we have detailed countermeasures for detection using only



* This figure describes representative data. There are actually other attributes that are changed due to file handling, such as the NTFS metadata entry allocation map (MFT Entry Bitmap).

Figure 13: File Referencing Mechanisms and Anti-Forensic Techniques on Windows NTFS File Systems

*62 "Backdoor.Prioxer!inf: 'Accidentally' the Stealthiest File Infector Ever!" (http://www.symantec.com/connect/ja/blogs/backdoorprioxerinf-accidentally-stealthiest-file-infector-ever).

*63 Methods of obtaining normal hash values for system standard executables include calculating them in advance using a PC that is not infected or downloading a public hash value database. For example, NIST (National Institute of Standards and Technology) publishes a database that includes hash values for the executables of major OSes. "National Software Reference Library" (http://www.nsrl.nist.gov/new.html).

*64 Malware that only infects memory cannot continue to operate after a PC is rebooted, but also cannot be detected using the disk analysis techniques presented here because it leaves no traces on the disk. The technique known as memory forensics that analyzes data in memory is effective when dealing with this kind of malware.

the information within a terminal, but the chance of detecting an infection early is increased if communications over the network are also examined for abnormalities.

1.4.3 Circumstances Surrounding the Great East Japan Earthquake

The Great East Japan Earthquake that occurred on March 11 was a catastrophic disaster that caused great loss of life and local infrastructure due to the major earthquake followed by tsunami and a nuclear power station accident. This disaster affected not only the Tohoku district*65 where the disaster struck, but also the Tokyo metropolitan district*66 and other outlying areas, though not on the same scale. Major disruption was caused to lifelines such as power, gas, and the water supply, as well as public transportation systems and the distribution of goods including basic commodities and gasoline.

Here we examine activities related to this disaster, such as Internet-based communication status and associated activities, aid-related information that tends to get buried amongst daily reports on the disaster, and attacks connected to the earthquake.

■ Status of Communications Following the Disaster

After the earthquake struck, abnormal states of communications were observed in Japan and on the Internet. Communications and power facilities in the area struck by the disaster were damaged by the earthquake and tsunami, making normal communications impossible. There were also reports of damage to international submarine cables*67. Additionally, restrictions were temporarily placed on outgoing calls from land lines and mobile phones in the Tokyo metropolitan district due to the large volume of calls from those wishing to confirm the safety of their relatives, rendering these lines of communication unusable.

Under these circumstances communication methods that allow information to be accumulated on servers such as email, Twitter, and Facebook were invaluable for confirming the safety of others, and some companies used Twitter to contact employees*68 to utilize such accumulation. Meanwhile, it was also pointed out that SNS played a role in spreading large amounts of unreliable information that did not specify sources*69.

Also, although a drop in the volume of Internet communications was observed immediately after the earthquake, access from those seeking up-to-date information was concentrated on specific Web servers such as those of local public bodies and power companies, leading to some becoming temporarily inaccessible. The situation did not return to normal in the week following the disaster, with many companies deciding to have employees work from home because of those forced to walk home when public transportation systems were suspended on the day of the earthquake, and because transportation systems were expected to remain unreliable over the following week.

From the week after the earthquake struck, IT systems such as Web servers in buildings with no emergency power system were often interrupted due to rolling blackouts. Despite this post-earthquake situation multiple incidents occurred on the Internet as per normal, and it was necessary to maintain vigilance regarding malware and vulnerability countermeasures.

*65 See the following New York Times summary for details regarding the area directly affected by the earthquake. “Map of the Damage From the Japanese Earthquake” (http://www.nytimes.com/packages/flash/newsgraphics/2011/0311-japan-earthquake-map/index.html?ref=europe).

*66 This refers to Tokyo and prefectures within commuting distance from Tokyo, such as Saitama, Chiba, Kanagawa, Ibaraki, Tochigi, Gunma, and Yamanashi. The population of this area is 42,920,000 according to Chapter 2, Section 1, “Population Status, etc.”, of the Tokyo Metropolitan District White Paper published by the Ministry of Land, Infrastructure, Transport and Tourism (http://www.mlit.go.jp/hakusyo/syutoken_hakusyo/h22/h22syutoken__files/zenbun.pdf) (in Japanese).

*67 See the following Network World report for information regarding the damage to international submarine cables. “Quake damage to Japan cables greater than thought Service is cut off on two segments of a trans-Pacific network” (http://www.networkworld.com/news/2011/031411-quake-damage-to-japan-cables.html).

*68 For example, at IBM Japan the following announcement was made to IBM group employees. “Request for employees to use Twitter for earthquake-related information” (http://www-06.ibm.com/jp/news/2011/03/1402.html) (in Japanese).

*69 For example, some information related to the nuclear power station accident suggested that drinking mouthwash would lessen the effects of exposure to radioactive materials, resulting in a warning being published by the National Institute of Radiological Substances. “Liquids such as disinfectant containing iodine should not be consumed - be wary of baseless claims spreading on the Internet” (http://www.nirs.go.jp/data/pdf/youso-3.pdf) (in Japanese).

Efforts toward Assisting Reconstruction and Rectifying the Status of Communications

In the aftermath of the earthquake multiple companies were involved in providing direct assistance such as relief supplies and donations to the quake hit area, as well as free use of message board systems for confirming the safety of individuals and software such as commercial OSes and map applications. Those in the disaster area were also granted exemption of service fees and free use of cloud servers*70. Likewise, there were many cases of action being taken to organize communications for distributing information appropriately. This includes the appearance of sites providing a comprehensive summary of useful information regarding earthquake response collected from various sources on the Internet*71, cloud servers being provided to websites unable to distribute information effectively due to concentrated access or damage from the disaster, and the mirroring of content. Additionally, there was a series of TV and radio retransmitted broadcasts on the Internet in order to communicate accurate information to the maximum number of people.

It was recommended that text or CSV formats be used instead of or in addition to file formats that tend to be large in size in comparison to the content (PDF and formats used by applications such as Excel) for the publication of information*72. At the same time, official government agency-related information began to be distributed over SNS such as Twitter and Facebook*73. Meanwhile, the Ministry of Internal Affairs and Communications requested that unconfirmed information spreading over the Internet (false rumors, etc.) be voluntarily deleted by ISPs from bulletin boards, blogs, etc.*74

Direct support from overseas was also provided to the disaster-hit area, such as disaster relief teams, relief supplies, and donations. Additionally, overseas product vendors in particular gave special consideration to Japan's state of communications. Microsoft excluded Japan from the official release of Internet Explorer 9 that was planned for March 14 U.S. time in order to reduce the load on Japan's network following the disaster*75. Cisco, a vendor for the routers used by many network companies such as ISPs, announced they were delaying their regular twice yearly firmware update (planned for March 23 U.S. time) by six months in consideration of Japanese ISPs that were focused on maintaining communications after the earthquake*76.

Attacks Linked to the Disaster

Meanwhile, attacks taking advantage of this disaster also occurred. First, immediately after the disaster there were SEO poisoning incidents targeting the earthquake in Japan and attacks originating from content designed to infect users with

*70 See the following for details regarding the reconstruction assistance activities of companies. Advanced Information Systems and Software Division, Information and Communications Bureau, Ministry of Internal Affairs and Communications "Status of Public and Private Initiatives in the Field of ICT regarding the Great East Japan Earthquake" (http://www.soumu.go.jp/main_content/000112455.pdf) (in Japanese). IIJ provided cloud environments for the transmission of information to the affected area and schedulers free of charge, announced exemption of its service fees through April 2011 to individual users in the quake-hit area, and also provided mirror sites for local authorities there (http://www.iij.ad.jp/news/pressrelease/2011/0316.html) (in Japanese).

*71 The government response included the disaster control site of the office of the Prime Minister (http://www.kantei.go.jp/saigai/) (in Japanese). Private sector initiatives included those from search service providers Google (http://www.google.co.jp/intl/en/crisisresponse/japanquake2011.html) and Yahoo! (http://notice.yahoo.co.jp/emg/en/).

*72 Local Authorities Systems Development Center "Regarding the file formats of important information distributed to citizens" (https://www.lasdec.or.jp/cms/12,22060,84.html) (in Japanese). The Ministry of Economy, Trade and Industry also published a similar announcement. "Regarding data formats for providing information regarding the Tohoku Region Pacific Coast Earthquake" (http://www.meti.go.jp/policy/mono_info_service/joho/other/2011/0330.html) (in Japanese).

*73 For example, information is provided via Twitter through the official accounts of the office of the Prime Minister (disaster information) (@kantei_saigai), the Ministry of Defense (disaster information) (@bouei_saigai), and the Fire and Disaster Management Agency, Ministry of Internal Affairs and Communications (@FDMA_JAPAN). Information is also provided mostly in English on the official site of the office of the Prime Minister on Facebook (http://www.facebook.com/Japan.PMO). Additionally, the Ministry of Economy, Trade and Industry lists confirmed government and local authority Twitter accounts as well as guidelines and policies for public institutions operating a Twitter account on their Social Media Portal for Public Institutions (http://smp.openlabs.go.jp/) (in Japanese).

*74 Following the Cabinet Secretariat Working Team on Measures to Ensure Safety and Peace of Mind in the Disaster Area published "Measures to Ensure Safety and Peace of Mind in the Disaster Area" (http://www.cas.go.jp/jp/seisaku/hisaitiwg/honbun.pdf) (in Japanese), the Ministry of Internal Affairs and Communications published "A Request to Telecommunication Carrier Organizations regarding the Appropriate Response to False Rumors about the Great East Japan Earthquake on the Internet" (http://www.soumu.go.jp/menu_news/s-news/01kiban08_01000023.html) (in Japanese). As an example of the response to this request, the Telecom Services Association published "Provision of information regarding responses to false rumors regarding the Great East Japan Earthquake on the Internet" (http://www.telesa.or.jp/taisaku/) (in Japanese).

*75 Microsoft "Regarding postponement of the Japanese product release of Internet Explorer (R) 9 due to the Tohoku Region Pacific Coast Earthquake" (http://www.microsoft.com/japan/presspass/detail.aspx?newsid=3969) (in Japanese). Distribution of the Japanese version of IE9 began on April 26. "Japanese version of Windows (R) Internet Explorer (R) 9 released" (http://www.microsoft.com/japan/presspass/detail.aspx?newsid=3995) (in Japanese).

*76 "Cisco Security Advisories and Notices, March 2011 Bundled Publication Deferred" (http://www.cisco.com/en/US/products/products_security_advisories_listing.html).

malware*77. It has been reported that many domains containing English words such as Japan, Earthquake, and Tsunami were acquired for this reason. After the earthquake occurred many of these attacks used English search key words and content such as photos of the affected area or videos of the tsunami, so it is thought that they were targeted at non-Japanese people who had an interest in what was happening in Japan*78. Although this type of attack exploits the high profile nature of such disasters, new attacks were being discovered even a month after the Great East Japan Earthquake struck.

Incidents in Japan in which the Japanese people were targeted include a chain email relating to the earthquake*79 that started a week or two after the disaster, donation fraud using telephone and email to impersonate public agencies, and phishing involving redirection to a fraudulent donation site, with warnings issued as a result*80. During the same period targeted attacks via email that utilized information related to the earthquake and nuclear power station were also confirmed*81.

Summary

At the time of writing aftershocks are still occurring, and it may be premature to summarize the related trends with the threat of this disaster still ongoing. However, as shown here Japan's Internet and communications situation has been affected by the disaster and continues to undergo change, still remaining volatile. It is also possible that attacks taking advantage of this crisis will continue in the future, and we would recommend readers be aware of the occurrences of attacks and stay informed about relevant information.

1.5 Conclusion

This report has provided a summary of security incidents to which IIJ has responded. This time we introduced our new observation environment, gave an overview of malware anti-forensics, and discussed the impact of the Great East Japan Earthquake on Japan's communication circumstances as well as related attacks.

In closing we would like to send our warmest regards to all those who are striving to provide relief to disaster victims and rebuild, and to the international community for the aid and cooperation they have given. IIJ will also continue its efforts towards reconstruction.

Authors:
Mamoru Saito
Manager of the Office of Emergency Response and Clearinghouse for Security Information, IIJ Service Division. 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. He is also active in multiple organizations such as the Council for Stable Operation of the Internet, and the Engineers SWG of the Working Committee for Child Pornography Countermeasures in the Association for Promoting the Creation of a Safe Internet.

Hirohide Tsuchiya (1.2 Incident Summary)
Hirohide Tsuchiya, Hiroshi Suzuki, Tadaaki Nagao (1.3 Incident Survey)
Hiroshi Suzuki (1.4.1 The Dionaea Honeypot)
Takahiro Haruyama (1.4.2 Malware Anti-Forensics)
Mamoru Saito (1.4.3 Circumstances Surrounding the Great East Japan Earthquake)
Office of Emergency Response and Clearinghouse for Security Information, IIJ Service Division

Contributors:
Masahiko Kato, Masafumi Negishi, Yuji Suga, Tadashi Kobayashi, Hiroaki Yoshikawa, Seigo Saito
Office of Emergency Response and Clearinghouse for Security Information, IIJ Service Division

Yoshinobu Matsuzaki, Network Service Department, IIJ Service Division

*77 Details of SEO poisoning incidents related to the disaster can be found in the following Trend Micro malware blog post. "3/11 Japan Earthquake Disaster Scam Watch" (http://blog.trendmicro.com/most-recent-earthquake-in-japan-searches-lead-to-fakea/).

*78 The following Kaspersky Lab blog post details the timeline of incidents occurring after the disaster from an international perspective. "The Japan crisis – an IT security timeline" (http://www.securelist.com/en/analysis/204792173/The_Japan_crisis_an_IT_security_timeline).

*79 The Anti-Spam Consultation Center was one of the organizations warning of the spam and chain emails related to the disaster (http://www.dekyo.or.jp/soudan/eq/index.html) (in Japanese).

*80 For example, Consumer Affairs Agency "Beware of Donation Fraud relating to the Earthquake" (http://www.caa.go.jp/jisin/110318gienkinsagi.html) (in Japanese), or the Council of Anti-Phishing Japan "Phishing under the guise of donations to Japan (3/14/2011)" (http://www.antiphishing.jp/news/alert/2011314.html) (in Japanese).

*81 Details can be found in the following IBM Tokyo SOC Report. Tokyo SOC Report "Trends in recent targeted attacks detected by Tokyo SOC" (https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/targeted_attack_20110324?lang=en_us) (in Japanese).

Why Japan Became the 3rd Largest Regional Source of Spam

In this report we will present an overview of spam trends for week 1 through week 13 of 2011.
China was the top regional source of spam. Japan's ranking rose steeply, climbing to 3rd place overall.
Here we examine the reasons for this, and discuss the current relationship between anti-spam measures and IPv6 addresses.

2.1 Introduction

In this report we discuss the latest trends in spam and email-related technologies, and summarize various activities in which IIJ is engaged. In this volume we focus on data for the period of 13 weeks from week 1 of 2011 (January 3 to January 9, 2011) to week 13 (March 28 to April 3, 2011), which corresponds to the 4th quarter for many Japanese companies. We also report on trends in authentication results ratios to gain insight into the adoption of SPF (Sender Policy Framework) sender authentication technology. Additionally, we touch on guidelines for the use of IPv6 addresses, which is expected to increase with the exhaustion of IPv4 addresses, as well as anti-spam measures.

2.2 Spam Trends

In this section, we will report on historical ratios of spam and the results of our analysis concerning spam sources based on trends detected by the Spam Mail Filter provided through IIJ's email services. In the previous report we noted that despite the downward trend in spam ratios in the latter half of last year, there were indications that they would increase again after the turn of the year. We provide a follow-up in this report.

2.2.1 Spam Decreases Sharply due to Suspended Rustock Activity

Spam ratios dropped precipitously at the end of last year, but began returning to their previous levels from the start of 2011. However, there was another abrupt drop in the ratio of spam in mid-March. Figure 1 shows spam ratio trends over the period of one year and three months (65 weeks), including the current survey period and the same period for the previous year.

The average spam ratio for the current survey period was 65.4%. This represents a drop of 6.7% over the previous report, and a significant drop of 16.7% over the same period for the previous year.

As mentioned in the previous report, it is thought that the decrease in the volume of spam in the latter half of last year is in part due to a drop in the activity of botnets that are the major sources of spam. The suspended activity of the Rustock botnet that accounts for a large portion of spam sent seems to be a primary factor. In the March edition of the

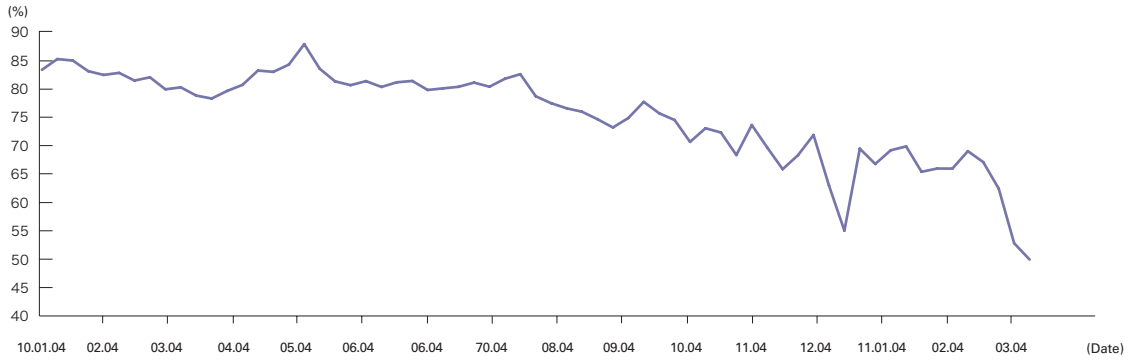


Figure 1: Spam Ratio Trends

Wall Street Journal Online*1, it was reported that Rustock activity was almost completely shut down due to Microsoft Corporation and federal law enforcement agents seizing the host computers controlling it*2. A similar account was published on the Official Microsoft Blog*3.

It is crucial for individual users to take steps to prevent their PCs from being incorporated into a botnet, and for PCs that may have been compromised to be cleaned swiftly. However, as demonstrated by the McColo network shutdown in 2008, finding a way to deal with the controller (herder) of bot PCs is an effective method of stopping botnet activity. If nothing else, it is clear from this example that it has a dramatic effect on spam.

2.2.2 Japan Becomes the 3rd Largest Regional Source of Spam

Figure 2 shows our analysis of regional sources of spam over the period studied. China (CN) was the number one source of spam in this survey, accounting for 12.4% of total spam. This is the first time China has taken the top spot since the 1st quarter of 2010. 2nd in the rankings at 8.0% was the United States (US), which had held the top position up until now. Japan (JP) was 3rd at 6.4%, which is the highest ratio and ranking it has held. The Philippines (PH, 6.1%) was 4th, India (IN, 5.8%) was 5th, and Russia (RU, 5.1%) was 6th.

Figure 3 shows week-to-week changes in ratios for the top 8 regions during the current period. China (CN) maintained a high ratio throughout this entire period, making it clear they were the number one source overall. The ratio for the United States (US), which was 2nd in rank, dropped after mid-January. It is difficult to see the characteristics from the ratio trends, but the period after mid-March when Rustock activity subsided also saw a large drop in actual numbers. The same trend can be seen in India (IN) and Brazil (BR). Meanwhile, the ratio for the Philippines (PH) rose significantly from the second half of February. The ratio for China (CN) also increased abruptly from March.

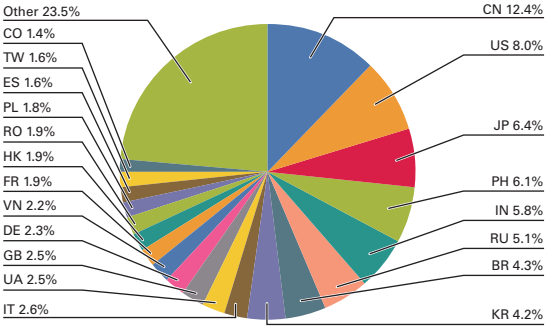


Figure 2: Regional Sources of Spam

2.2.3 Regional Characteristics of Spam Sources as Demonstrated by the Suspension of Rustock Activity

The ranking and ratio of spam originating from Japan rose from 5th place (4.7%) in the previous period. However, comparing numbers with the previous report and the same period for the previous year, there was no significant increase in the actual volume of spam sent. It is thought that the increase in the ratio for Japan is in part due to a drop in the activity of botnets such as Rustock. Figure 4 shows how ratios for the top 8 regions have changed compared to the same period for the previous year (week 1 to week 13 of 2010).

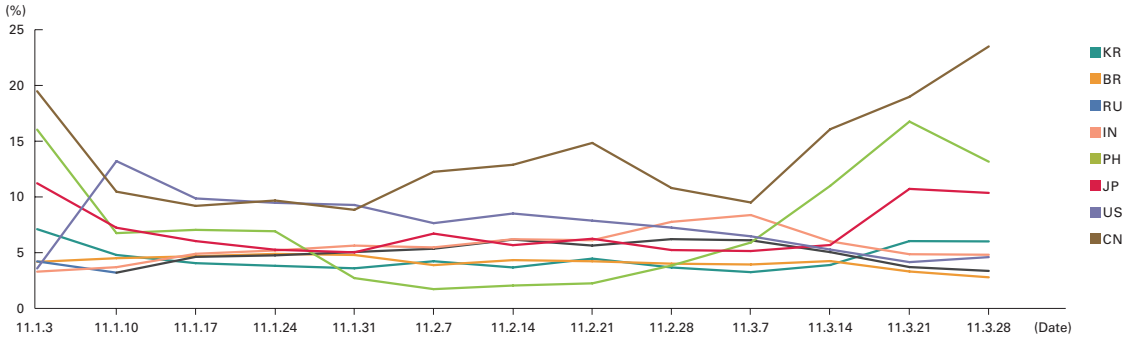


Figure 3: Trends in Ratios for the Main Regional Sources of Spam

*1 The Wall Street Journal (http://online.wsj.com/public/page/news-tech-technology.html).

*2 Botnets involve PCs being infected with malicious programs, with said PCs then being controlled via an external host to conduct activities such as the sending of spam.

*3 The Official Microsoft Blog (http://blogs.technet.com/b/microsoft_blog/archive/2011/03/17/taking-down-botnets-microsoft-and-therustock-botnet.aspx).

The figure shows ratios for China (CN), Japan (JP), and Russia (RU) at about 80% of those for the same period the previous year, demonstrating that spam volumes have not dropped significantly. On the other hand, ratios for the United States (US), India (IN), and Brazil (BR) have dropped to below 50%, leading us to believe that the Rustock botnet was active in these regions.

We can also confirm the relationship between botnets and spam volume by examining the Internet environment in Japan. As we have stated several times in the past, Japan has always had low volumes of spam originating from botnets due to the widespread implementation of OP25B*4. In other words, because Japan remained largely unaffected by the shutdown of Rustock, there was little actual decrease in spam volume, with numbers at about 80% of those for the same period of the previous year. Similarly, we believe that the small decrease seen for China (CN) and the large increase in volume sent from the Philippines (PH) point to methods other than the Rustock botnet being used, at least with regard to spam sent to Japan. As mentioned in the previous report, it has been reported several times that Japanese spammers are based in these regions. Regarding geographically isolated Russia, we currently believe it likely that a botnet other than Rustock has spread there.

2.3 Trends in Email Technologies

Here we will examine a variety of technological trends relating to email. In this report we will continue to look at trends in the recipient authentication results for sender authentication technology. We also summarize the current state of the relationship between anti-spam measures and IPv6 addresses.

2.3.1 Volume-Based SPF Authentication Result Ratios

Figure 5 shows SPF authentication result ratios for email received during the current survey period (January to March 2011). As with the previous survey 50.2% of authentication results showed “none,” indicating that the sender domain did not declare an SPF record. The 28.6% ratio of authentication results that showed “pass” was a 5% increase over the previous period. In contrast, the total ratio of results showing “hardfail,” “softfail,” or “neutral” that indicate an authentication failure fell 4.7% compared to the previous period. We believe the increase in successful SPF authentication results is due to the drop in spam ratios and the rise in the ratio of email from legitimate sources that have implemented SPF. Meanwhile, we think the reason that the overall implementation ratio has not increased comes down to the fact that the ratio of spam using the sender information of domain names that have implemented SPF and the ratio of spam not implementing SPF are at comparable levels. In other words, we can surmise that at least with regard to the decreased volume of spam, about half of the domains had already implemented SPF. The decrease in the ratio of authentication failures may point to misrepresentation using legitimate domain names, but considering the drop in spam ratios we believe that a considerable volume of spam openly implements SPF to pass authentication.

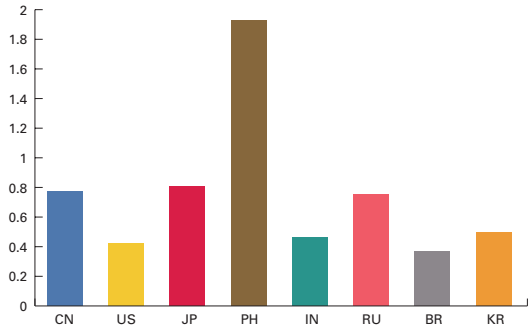


Figure 4: Previous Year Comparison of Major Regional Sources of Spam

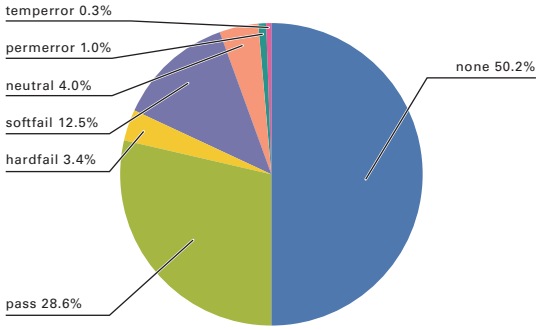


Figure 5: SPF Authentication Result Ratios

*4 OP25B (Outbound Port 25 Blocking) is technology that prevents the dynamic IP addresses used for the Internet connections of consumers from accessing port 25, which is used to connect the mail servers of external networks. It is said to suppress the sending of spam.

2.3.2 Anti-Spam Measures and IPv6

On April 15 as this report was being written, JPNIC announced*5 that the IPv4 addresses available at APNIC and JPNIC for allocation by standard application had been exhausted. Because of this, it is expected that the use of IPv6 addresses will increase. For this reason, we will summarize the relationship between anti-spam measures and IPv6 addresses here.

First, we will discuss the relationship between sender authentication technology and IPv6 addresses. DKIM (DomainKeys Identified Mail) carries out authentication using digital signatures, and because it does not rely and the sender's IP address, there is no impact when sending or receiving email using IPv6 addresses. The SPF records used by SPF and SenderID already include a specification that supports IPv6 addresses. When IPv6 is used for the sender's IP address, "ip6" is added to the SPF record as a mechanism, so there are no issues as long as an IPv6 IP address or network address is added.

Next, we will look at the relationship between frequently used anti-spam measures and IPv6. One function commonly used in anti-spam measures is the content-based detection of spam through email characteristics. As this involves detecting spam from the content of an email, IPv6 has almost no impact.

Another anti-spam measure is the detection of spam based on the sender's IP address. This includes assessing corresponding IP addresses based on a black list, and greylisting in which it is expected that email from a source IP address not identifiable as a threat will be resent. These methods may appear workable provided a database that supports IPv6 addresses is prepared. However, this brings about serious operational issues. Namely, the fact that the IPv6 address space is vastly larger than that of IPv4. Technically, this makes it possible to send a significantly large volume of spam, even if it requires changing the source IPv6 address for each email. When using previous methods such as DNSBL that detect whether or not mail is a threat according to individual IP addresses, it seems highly unlikely that it would be possible to properly manage spam sources. Consequently, we believe that managing IPv6 addresses consolidated to a certain degree by network address would be preferable to managing them individually using a black list. However, when a large range is consolidated together it may also include legitimate mail servers, so care must be taken. Conversely, a white list method of operation whereby all IPv6 addresses are treated as threats and a list of legitimate mail servers with proper anti-spam measures in place is managed could also be a viable option. However, the number of legitimate mail servers existing on the Internet is an unknown quantity, so a significant period of trial and error may be required to generate a suitable list of IP addresses.

Most mail services provided by IIJ already allow the receipt of mail sent from IPv6 addresses. We plan to report on the status of these mail services and the relationship between IPv6 and email in the future.

2.4 Conclusion

We would like to express our heartfelt sympathy to those affected by the Great East Japan Earthquake. We pray for the quick recovery of the quake-hit zone. The distribution of information is extremely important during times of crisis. It goes without saying that email and the prevalence of mobile phones, as well as their immediacy and the asynchronous nature of the messages that are exchanged, are invaluable for distributing information. We would like to continue to play a role in providing Internet services that facilitate the distribution of information, as well as email applications widely used on this infrastructure, and we will strive to provide solutions that remain available even when disasters such as this strike.

Author:
Shuji Sakuraba
Mr. Sakuraba is a Senior Engineer in the Application Service Department of the IIJ Service Division. He is engaged in the research and development of messaging systems. He is also involved in various activities in collaboration with external related organizations for securing a comfortable messaging environment. He is a MAAWG member and JEAG board member. He is a member of the Council for Promotion of Anti-Spam Measures and administrative group, as well as chief examiner for the Sender Authentication Technology Workgroup. He is also a member of Internet Association Japan's Anti-Spam Measures Committee. He is a member of the Ministry of Internal Affairs and Communications' Unsolicited Mail Measure Working Group.

*5 Regarding the exhaustion of IPv4 addresses (http://www.nic.ad.jp/ja/ip/ipv4pool/) (in Japanese).

Web Access Consolidation and Access Pattern-Based Optimization for Web-based Service Platforms

At the Research Laboratory we are conducting research into the use of Web-based Service Platforms in cloud infrastructure as part of research and development for next-generation cloud solutions. In this report we discuss Web server optimizations based on the consolidation of Web access and access patterns, which are the key to achieving high scalability and resource utilization for Web-based Service Platforms.

3.1 Web Server Resource Design

Typical Web server construction involves forecasting website request numbers and traffic volume and estimating the necessary content throughput, before estimating system resources and designing the server configuration based on this data. Web access variation is taken into account when making these forecasts.

There are two main variation patterns for Web access. The first is a cyclical variation pattern that occurs on a daily or weekly basis. The second is a variation pattern based on concentrated access. Concentrated access can be caused by a variety of factors. Some examples include news releases, game or software releases, links from the top page of major news sites, and URL captions on TV.

Because Web access can surge suddenly due to concentrated access, variations in Web access are taken into consideration during Web server resource design and backup resources added to estimates (over-provisioning). As shown in Figure 1, when implementing resource design using over-provisioning, the more backup resources that are added to the estimate in preparation for concentrated access, the lower the utilization of Web server resources will be.

Because Web services account for a large percentage of data center and cloud services, improving the resource utilization of Web servers also leads to improved overall resource utilization for data centers and cloud solutions.

3.2 Improving Resource Utilization through Web Access Consolidation

Many websites experience concentrated access following events with significant social impact such as the recent Great East Japan Earthquake. However, it is generally accepted that concentrated access will occur at different times for individual websites. This is because the causes of concentrated access and extent of its impact are both limited. Assuming that concentrated access occurs randomly at individual websites in accordance with probabilistic distribution, by consolidating traffic for multiple websites it stands to reason that the probability of concentrated access occurring over this consolidated web access would increase in proportion to the number of consolidated services. We therefore envisaged that it would be possible to reduce the overall variation in Web access by exploiting the fact that consolidated Web access raises the probability of concentrated access occurring. In other words, this would mask the variance in Web access due to concentrated access by intentionally creating a Web access environment that constantly faces concentrated access.

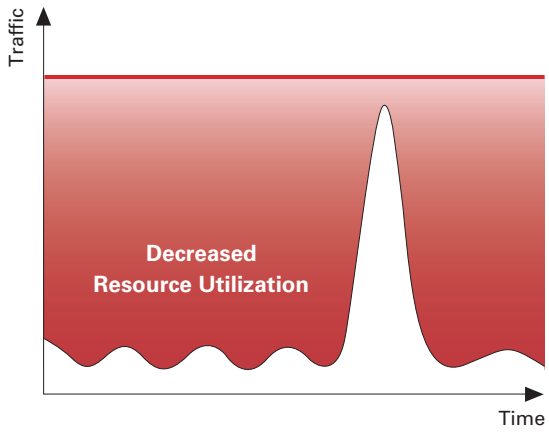


Figure 1: Decreased Resource Utilization through Over-Provisioning

To verify this concept we simulated a consolidated Web access environment in which concentrated access occurred at random, and observed the impact of individual pockets of concentrated access as well as the overall variance in access volume. The results are shown in Figure 2. The bottom graph shows the variance in Web access volume when Web services are not consolidated. The other three graphs show the variance in Web access volume when 10, 100, and 1,000 websites are consolidated, respectively.

The sharp spikes in these graphs indicate concentrated access. To make it easier to see the variance in access volume due to concentrated access as well as its impact, we have not included variance patterns for cyclical Web access.

The simulation results showed that consolidating Web access during concentrated access that occurs on a sporadic basis at individual sites led to comparatively less overall impact from access variance due to individual pockets of concentrated access. From this we believe it will be possible to smooth out Web access variance through the consolidation of Web access.

Next we will examine the merits of consolidating Web access with regard to resource design. Because consolidation masks and smoothes out the access variance resulting from concentrated access, resource design for consolidated websites can be implemented based on Web access with less variance. As shown in Figure 3, we believe this means that it will be possible to free up backup resources previously retained on an individual website basis, and lower the overall estimated backup resources required. For this reason we believe that it will be possible to improve the overall resource utilization of websites by consolidating them and basing the resource design on this.

3.3 Access Variance for Popular Content

We believe that higher efficiency for Web servers will be made possible through improving the processing efficiency of requests to consolidated Web access environments. We are looking at adapting request processing to Web access patterns as one method of implementing this.

Because concentrated access occurs on the Web due to certain limited factors, the content where access is concentrated is also limited. For this reason, when Web access is consolidated access will be concentrated on a fixed percentage of specific content. It should be possible to improve Web server optimization through the efficient processing of requests for the content where access is concentrated.

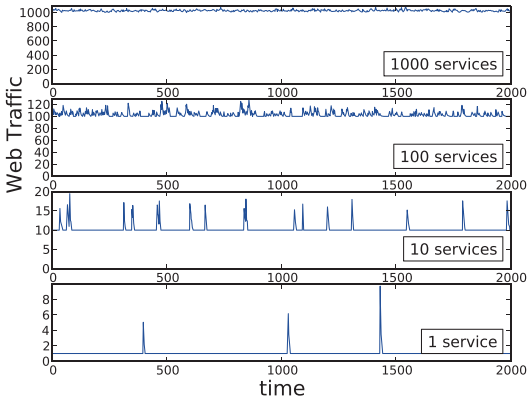


Figure 2: Differences in Web Access Variations due to Website Consolidation

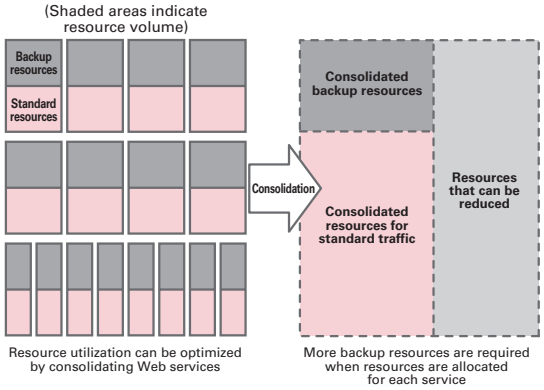


Figure 3: Backup Resource Reduction due to Website Consolidation

The content where access is concentrated is not always the same, and will shift over time. To process these requests efficiently it is necessary to consider the degree that access is concentrated on a given of piece content as well as changes in this concentration. To this end we analyzed content where access was concentrated based on the actual traffic logs of Web servers. For this analysis we used traffic logs for the Web servers of the Japan Advanced Institute of Science and Technology (JAIST). JAIST operates the largest Web service for the distribution of free software in Japan, resulting in a large number of users converging there. It is also the largest domestic distribution site for Firefox, so concentrated access can be predicted to accompany software releases.

Figure 4 is a graph indicating the cumulative distribution function (CDF) of content, traffic volume, and requests in order of peak requests for each piece of content based on a random sampling of 17,000 pieces of content, accounting for approximately 2% of the content requested over the course of a certain month at JAIST. Traffic and requests are the total number for each piece of content over the period of analysis (180 days). From the cumulative distribution function of content (the green dashed line) in this figure, we can see that approximately 90% of the peak requests for content amounted to less than 10^2 (100) requests per day. However, looking at the cumulative distribution function for traffic (red line) and requests (blue line) in the figure, it is clear that content with peak requests of less than 10^2 (100) requests per day accounted for a tiny percentage of approximately 2% of traffic and requests. This points to the fact that access is skewed towards content with more than 10^2 (100) peak requests per day.

Based on these results, we analyzed changes in the concentration of access for content receiving more than 200 requests per day. We identified the number of requests per day for each piece of content over the analysis period of 180 days, and labeled the highest value as the day that requests peaked. Additionally, in order to analyze the variation in requests for a period of 10 weeks after peak, we elected to use only data for which the day that requests peaked was at least 70 days before the end of the analysis period. As a result, we gathered data on approximately 3,000 pieces of content meeting the criteria.

Figure 5 and Figure 6 show the peak requests as well as changes in the number of requests for each piece of content 1 day and 7 days after requests peaked. The horizontal axes of these figures show the number of requests for the content on the day that requests peaked. The closer to the green line, the less change was observed in the number of requests after requests peaked. Content for which the number of requests fell to 0 either 1 day or 7 days later were recorded as 10^{-1}.

The spread of red dots on these figures indicates the drop in the number of requests compared to the peak requests. Comparing results for 1 day and 7 days later, the spread of points is wider for 7 days later, showing that for most content the more days that pass after requests peak, the greater the decrease in requests will be. Following the same

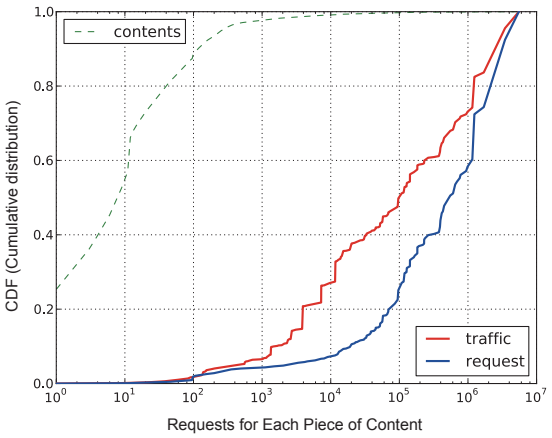


Figure 4: Content, Requests, and Traffic Share based on Peak Requests for Each Piece of Content

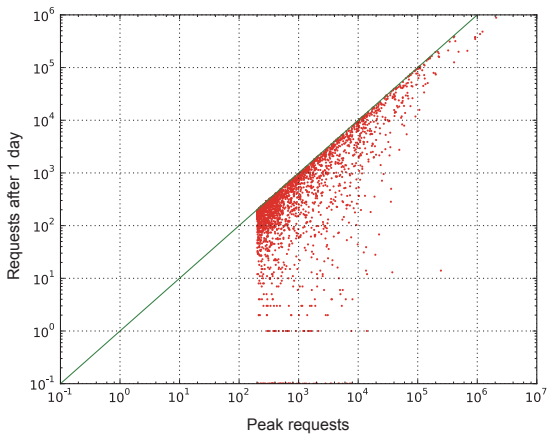


Figure 5: Changes in Requests for Each Piece of Content (1 Day Later)

method, we compared changes in the number of requests over 10 weeks on a weekly basis. In this case the spread of points stopped gradually, showing that after 4 weeks requests continued to be received for a certain amount of content even when 10 weeks passed.

Using the same data, we also identified the rate of decline in requests from the day that requests peaked to 10 weeks later for each piece of content. Figure 7 shows the mean value (blue line) and median value (red dashed line) for the rate of decline in requests. From this figure, we can see that the number of requests was approximately 40% of the peak value about 1 week after the day that requests peaked, and this value continued to decline gradually thereafter. The slope of the median value is greater than that of the mean value, and approaches 0 first. In other words, it appears that the number of requests is declining faster than the average value for most content because the decline in requests is more gradual for some content, pushing the mean value up.

It is likely that the numerical results obtained here are unique to JAIST Web servers and do not apply to general Web services. However, we can consider this one pattern of variation in requests for content where access is concentrated. We believe that when consolidating Web access where concentrated access occurs on a constant basis, analyzing the behavior surrounding content such as this is crucial for evaluating the optimization of request processing on Web servers.

3.4 Conclusion

The information on Web access consolidation and optimization of request processing adapted to content access patterns presented here is currently still at the research stage, and we do not yet provide services based on these design concepts. However, this does not change the fact that Web services will continue to play a key role in information infrastructure. We believe that research and technological development aimed at expanding the scope of Web services using large-scale resources such as cloud computing will become more important in the future. We plan to continue this research as part of larger research goals such as these.

In closing, we would like to offer our sincerest thoughts and prayers to those who lost their lives in the recent earthquake. We pray for the swift recovery of those affected by this tragedy.

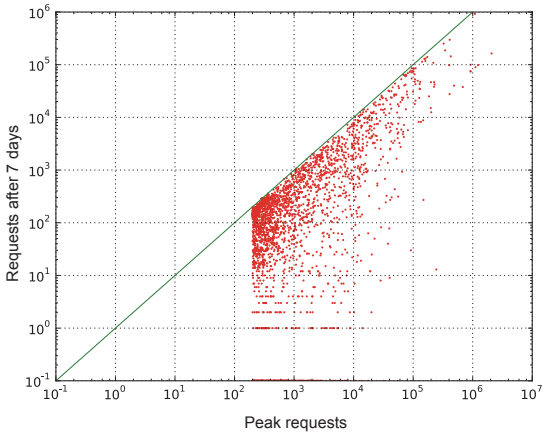


Figure -6: Changes in Requests for Each Piece of Content (7 Days Later)

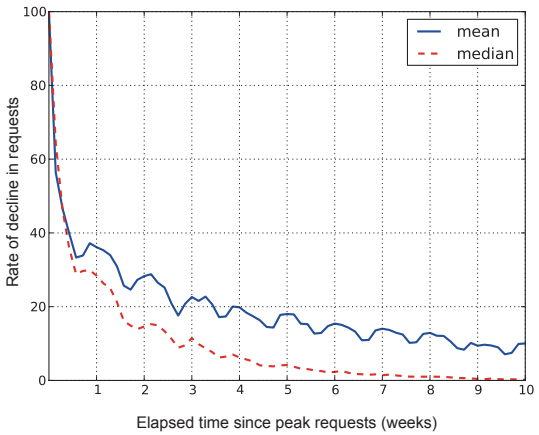


Figure 7: Rate of Decline in Access Numbers for Each Piece of Content

Author:
Megumi Ninomiya
Research Laboratory Research Associate, IIJ Innovation Institute Inc. Ms. Ninomiya is engaged in the research of Web-based Service Platforms with the goal of achieving high performance and high resource utilization for cloud infrastructure.

The IPv4 Address Exhaustion Issue and Guidelines for Response

On April 15, 2011, the regular pool of IPv4 addresses for the Asia-Pacific region was exhausted.
In order to continue using the Internet in the future as we have done up to this point,
we must respond appropriately to the IPv4 address exhaustion issue.
Here we examine the methods that should be used to deal with this issue.

4.1 Introduction

The growth of the Internet to date gives a sense of how wonderful it is to be connected via a network. It is now possible to keep in touch with different people all over the world from Japan, and we can send email and browse the Web as usual even when traveling as long as we have Internet access. Last year I had the opportunity to visit a number of regions around the world, and the hotels in each region provided wireless LAN and Ethernet ports for accessing the Internet, allowing me to carry out my work in the same manner as usual. The Internet is now used to optimize business activities and provide quick access to information.

It is also important to recognize that the Internet makes it easy to develop new services. There are many examples of emerging companies accomplishing rapid growth after developing new services such as those for voice calls or video distribution. I believe it is likely that the number of people and regions with access to the Internet will continue to increase worldwide, and new services will continue to be provided via the Internet. The issue this wonderful tool that is the Internet now faces is that international availability of the IPv4 addresses required to connect to the Internet is drying up. This is known as the IPv4 address exhaustion issue.

4.2 Asia-Pacific Region Status

The IP addresses used for Internet communications are currently allocated through Internet registries*1, which have a hierarchical structure. Under this hierarchical structure the global free pool of available IPv4 addresses is managed by IANA*2 (Internet Assigned Numbers Authority), which is operated by ICANN. IANA allocates IP addresses to RIR (Regional Internet Registry) established in each region. LIR (Local Internet Registry) such as ISPs that actually assign IP addresses to users receive IP address allocations via an RIR such as APNIC or an NIR (National Internet Registry) such as JPNIC. In the middle of the night on February 3, 2011 Japan time the central pool of IPv4 addresses was exhausted at IANA, which manages the global free pool of addresses. This was triggered by the allocation of two /8 blocks to APNIC, leaving five /8 blocks in the central pool at IANA, at which point the remaining IP addresses were allocated to the five RIR in accordance with a previously established policy.

Because the central pool of IPv4 addresses has been exhausted, availability at each RIR will dwindle as addresses are allocated. APNIC, which allocates IP addresses as RIR for the Asia-Pacific region, will cease regular allocation of remaining IPv4 addresses when down to its last /8 block, and will subsequently adopt a policy of allocating only one /22 block to each member organization. It was thought that regular allocation would end sometime during the summer of 2011. However, the free pool of IPv4 addresses at APNIC was actually reduced to one /8 block early than expected, on April 15, 2011. For this reason, APNIC has now transitioned to a policy for IPv4 allocation from the last /8 block. Because JPNIC, which handles IP address allocation for Japan, shares its pool of IPv4 addresses with APNIC, the allocation of IPv4 addresses in Japan has also finished. This means we are facing the exhaustion of IPv4 addresses ahead of other regions, so the eyes of the world are focused on what is happening in the Asia-Pacific region.

*1 Organizations that allocate and manage Internet resources such as IP addresses.
*2 A faculty for managing and regulating the Internet resources operated by ICANN.

The regular pool of IPv4 addresses have been exhausted in the Asia-Pacific region. Currently, the pool of addresses at organizations actually operating networks such as ISPs that receive IPv4 address allocations from APNIC or JPNIC are being consumed. The number of IPv4 addresses remaining and the speed of their consumption will vary for each ISP. However, at ISPs continuing to gain users and expand their services, remaining IPv4 addresses will be exhausted in the near future. If this issue is neglected there could be repercussions, such as ISPs not being able to accept new users or provide IPv4 addresses when they are required temporarily for the redesign of systems.

4.3 Responding to the IPv4 Address Exhaustion Issue

The Internet still has a wealth of untapped potential, and many people desire to maintain an environment that can be used by people in more regions of the world. The following three solutions could be considered in response to the IPv4 address exhaustion issue that we currently face.

- Raising the utilization rate of IPv4 addresses
- Sharing IPv4 addresses
- Migrating to IPv6

Currently the only effective way of dealing with the issue permanently is the third solution, migrating to IPv6. However, it is likely that while deploying IPv6 a combination of multiple solutions will be implemented depending on the status of the ISP and network.

4.3.1 Improving IPv4 Address Utilization

Improving IPv4 address utilization in response to this issue involves targeting IPv4 addresses that are no longer used due to changes in business and network configurations. This solution aims to extend the life of IPv4 by recovering IPv4 addresses that are no longer in use and redistributing them to other organizations that require them. However, recovering IPv4 addresses in small batches is not an effective solution. It may be possible to implement this in some form within organizations, but to properly maintain reachability over the Internet a block of sequential IPv4 addresses is required. At this point in time a size of approximately one /24 block is necessary. Additionally, although there have already been cases of IPv4 addresses being recovered, there are issues such as the difficulty of persuading the providing party, the length of time required for recovery, and high demand resulting in recovered addresses being used up immediately.

A policy for promoting the utilization of unused IPv4 addresses has also been discussed. This is called the IPv4 Address Transfer Policy. When following standard procedures, addresses that are no longer required are first returned to JPNIC or APNIC, and then redistributed to the organization that requires them. However, under this policy IPv4 addresses can be transferred between organizations provided that both parties reach agreement. JPNIC plans to implement a transfer system by around summer 2011. Also, because this policy was already implemented at APNIC last year, it is now possible to transfer IPv4 addresses within the range managed by APNIC. Because the policy for the transfer of IPv4 addresses only deals with confirming agreement between the providing and receiving parties, APNIC or JPNIC are not involved even when money changes hands. It is said that IPv4 address transfers amount to the buying and selling of IPv4 addresses. Because money is involved, it is more likely that IPv4 addresses will go to the organizations that need them. Transfer procedures have actually already been carried out in the United States.

4.3.2 Sharing IPv4 Addresses

The sharing of IPv4 addresses involves moving forward using the NAT technology that is already in use. Many homes currently have a NAPT router installed. Users are generally allocated a single IPv4 address from their ISP, with the number of addresses required reduced by sharing this address between internal hosts using NAPT. This solution involves taking this concept one step further, and having ISPs run a large-scale NAPT on their side to further reduce the number of addresses required. This would allow ISPs to provide connection services to more users using the IPv4 addresses they already have. However, this could lead to degradation in service. For example, because the IPv4 address allocated to a user would not be directly reachable via the Internet, there is a chance that games and

other applications could no longer be used from home, and that public Web servers would no longer be operable. Additionally, depending on the NAPT implementation features such as VPN may be limited.

4.3.3 Migration to IPv6

It is likely that responses to the IPv4 address exhaustion issue will involve using the solutions detailed above to extend the life of IPv4 while migrating to IPv6, which will dramatically increase the number of IP addresses available. To achieve this IPv6 connectivity must first be secured. In Japan the implementation of IPv6 was initiated comparatively quickly, and a number of ISPs already provide IPv6 connectivity. Companies can use these services to proceed with support for IPv6. Home use is currently stalled until access network support is in place. However, a number of providers have already indicated they will support IPv6, and an environment for providing access to IPv6 connection services is scheduled to be in place by the end of the year. It appears that for the foreseeable future those requiring IPv6 connectivity will need to apply for it, but in the future it should be possible to secure IPv6 connectivity as standard when signing up for a Internet connection that uses an access network compatible with IPv6.

Migrating from an IPv4-only environment to one that combines both IPv6 and IPv4 inevitably increases complexity. Moreover, accessing an IPv6 service from a device that only supports IPv4 or accessing an IPv4 service from an IPv6 device requires the implementation of a device for suitably mediating between these communications. In this case the mediating device handles the complexity resulting from combining IPv6 and IPv4, which should simplify processing on the terminal side. However, when a communications error of some kind occurs, isolating the problem becomes extremely difficult. This means this method can only be used at times when support is too difficult or when usage will be limited. The preferred method at this point in time is to move forward with support for IPv6 while IPv4 addresses can still be used, and then prepare an environment that can be accessed via both IPv6 and IPv4. In most implementations IPv6 connectivity will be used as priority, so the key will be to secure high quality IPv6 connectivity from day one.

4.3.4 Other Issues of Concern

There are other matters of concern with regard to IPv4 address exhaustion. If IPv4 addresses are transferred between organizations, information about who is managing those IPv4 resources will become even more important. In the past there have been problems with route hijacking where another party's IP address is advertised without permission. In most cases these issues were caused by incorrect settings. However, because at some point in the future available IPv4 address will run out, providing the opportunity to profit from IPv4 address transfers, it is conceivable that there may be cases in which another party's IPv4 addresses are used or transferred without permission by hijacking registered information. Organizations that manage networks such as ISPs must update the information registered to the Internet Registry correctly, and confirm than no unintended changes have been made to the registered information.

4.4 Conclusion

IPv4 address exhaustion is not a new problem, as it has been discussed for many years. It was initially thought that the implementation of IPv6 would take place more swiftly. However, in reality implementation is proceeding at a sluggish pace, and the exhaustion of available IPv4 addresses appears likely to come first. For this reason, it has become necessary to move ahead with implementing IPv6 while maintaining IPv4 connectivity, which is a higher cost solution. From this point forward, the longer migration to IPv6 takes, the greater the cost of development and device installation will be for maintaining IPv4 connectivity. We hope to see IPv6 implemented in the smoothest possible way, so the Internet becomes an environment where everyone can share their wisdom on more entertaining topics.

Author:
Yoshinobu Matsuzaki
Mr. Matsuzaki is a Senior Engineer in the Network Service Department of the IIJ Service Division. Mr. Matsuzaki is always finding things that pique his interest while striving at his work. He is an IIJ-SECT member, co-chair of The Asia Pacific OperatorS Forum, chair of APNIC IPv6 SIG, and an expert advisor for JPCERT/CC.

Internet Topics: World IPv6 Day

With the exhaustion of IPv4 addresses now a reality, the need for IPv6 is becoming more widely recognized. However, the implementation of IPv6 is not proceeding very rapidly. As devices are connected to the Internet via a variety of access environments around the world, it appears the impact of implementing IPv6 is difficult to gauge. This led to the creation of World IPv6 Day, in which well-known content providers take the initiative in performing worldwide IPv6 trials to promote IPv6 implementation and issues to a wide range of ISPs and related organizations. The first to announce their participation in the project were Google, Facebook, Yahoo!, Akamai, and Limelight Networks, with ISOC*1 (Internet Society) creating a website*2 for it. The outline of the project was determined through discussions between participating organizations and those assisting the project. A suitable day was chosen after the exhaustion of the central pool of IPv4 addresses managed by IANA.

From 9 AM on June 8, 2011 Japan time, content providers participating in World IPv6 Day will make their main content compatible with IPv6. In other words, an AAAA record will be added to the host name, and this state maintained over a period of 24 hours. Many sites from countries around the world have already agreed to participate, including several sites in Japan. On the day, an increased amount of content will be accessible using IPv6. In some respects it is unfortunate that there is still a need to implement IPv6 trials, despite the fact that many sites such as http://www.iij.ad.jp already support IPv6. However, we believe that there is value in organizing World IPv6 Day to promote the implementation of IPv6 across the globe.

In Japan, information about World IPv6 Day is provided via organizations such as JANOG*3 (JApan Network Operators Group), with details supplied and discussions held on April 13, 2011 in a meeting regarding World IPv6 Day trends and measures that was attended mainly by ISPs. We know that when users connect to a walled-garden IPv6 network, issues can occur depending on the PC implementation and the applications used. These issues can be avoided through application updates, etc., but even more important is providing a better IPv6 access environment to users to encourage active participation in World IPv6 Day. However, in Japan the methods for providing this are limited, so only a limited number of ISPs can provide IPv6 access in time. It is necessary to consider support measures such as recommending that users upgrade their software through user support, and making it possible to select a suitable protocol by changing the policy table. Additionally, some ISPs may need to look into measures for controlling AAAA record responses on DNS cache servers to avoid unnecessary fallback.

The website http://www.attn.jp/worldipv6day/ has been established to provide information about World IPv6 Day in Japanese, and the presentation materials from the meeting held on April 13 have also been made available. Additionally, an announcement promoting these activities jointly signed by the Internet Association Japan, the IPv6 Promotion Council, the Japan branch of ISOC (currently being reactivated), and the WIDE Project was sent out to member organizations as notice that World IPv6 Day is to be held. Those considering participating in World IPv6 Day should check the URL above as well as the ISOC website and then carry out registration procedures. We would also recommend that ISPs consider all possible measures in advance to limit the impact of any confusion on the day to a minimum.

The smooth implementation of IPv6 is an important issue and challenge for Internet usage. With World IPv6 Day fast approaching, participating organizations and cooperating groups are actively evaluating and implementing their preparations, measurements, and necessary responses. IIJ will also continue to cooperate with related organizations to ensure that this World IPv6 Day initiative is a success, and that future IPv6 implementation and World IPv6 Days are fruitful endeavors.

Author:
Yoshinobu Matsuzaki
Mr. Matsuzaki is a Senior Engineer in the Network Service Department of the IIJ Service Division.

*1 An international nonprofit organization established to take a lead role in Internet-related standardization, education, and policies.
*2 The ISOC (Internet Society) website for this project (http://isoc.org/wp/worldipv6day/).
*3 A group that discusses, evaluates, and introduces matters related to Internet technology and operations.

Ongoing Innovation

Vol.11 May 2011

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: Jinbocho Mitsui Bldg., 1-105 Kanda Jinbo-cho, Chiyoda-ku, Tokyo, 101-0051
Email: info@iij.ad.jp URL: http://www.iij.ad.jp/en/

IIJ-MKTG020IA-1106CP-00001PR