Continuing Attacks on Companies and Government-Related Organizations

In this report we examine the details of a series of attacks on companies and government-related organizations that have been occurring since the end of last year, and discuss guidelines for dealing with DDoS attacks at telecommunications carriers.

1.1 Introduction

This report summarizes incidents to which IIJ responded, based on general information obtained by IIJ itself related to the stable operation of the Internet, information from observations of incidents, information acquired through our services, and information obtained from companies and organizations with which IIJ has cooperative relationships. This volume covers the period of time from April 1 through June 30, 2011. In this period vulnerabilities related to Web browsers and their plug-ins continued to be exploited. There was also an increase in smartphone malware distributed as malicious applications, and a large-scale system failure in a South Korean financial system. There were continued attacks on a number of companies and government-related organizations around the world. 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 April 1 and June 30, 2011. Figure 1 shows the distribution of incidents handled during this period*¹.

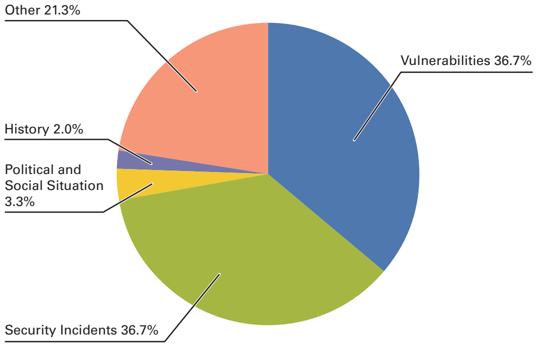


Figure 1: Incident Ratio by Category (April 1 to June 30, 2011)

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

Vulnerabilities

During this period a large number of vulnerabilities were discovered and fixed in Web browsers and applications such as Microsoft's Internet Explorer[*2][*3] and Windows[*4][*5][*6], Adobe Systems' Adobe Reader and Acrobat[*7][*8], Flash Player[*9][*10][*11][*12], and Shockwave Player[*13], Oracle's JRE[*14], and the WebGL[*15] standard specification for displaying 3D in Web browsers. Multiple vulnerabilities were also fixed in Apple's Mac OS X[*16][*17]. Several of these vulnerabilities were exploited before patches were released.

Many vulnerabilities were also patched in server applications, such as Microsoft's IIS (Internet Information Service)[*18], the Flash Media Server[*19] used for distributing Flash content, Oracle's Oracle Database[*20] used in database servers, the ISC BIND[*21] DNS server, the Apache HTTP Server[*22] Web server, and the CMS platform WordPress[*23]. Additionally, vulnerabilities were discovered and fixed in Apple's iOS[*24] platform for mobile phones and other devices.

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 assassination of Osama Bin Laden in Pakistan, the Japan-China-South Korea trilateral summit, and the G8 summit. However, IIJ did not detect any direct attacks on IIJ facilities or our client networks.

History

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

Security Incidents

Unanticipated security incidents not related to political or social situations included a large number of DDoS attacks on government agencies and companies as well as information leaks from servers perpetrated by multiple groups with distinct motives. See "1.4.1 Continuing Attacks on Companies and Government-Related Organizations" for more information about these incidents. The LizaMoon malware that alters websites using SQL injection attacks also

[*2] Microsoft Security Bulletin MS11-018 - Critical: Cumulative Security Update for Internet Explorer (2497640) (http://www.microsoft.com/technet/security/bulletin/ms11-018.mspx).

[*3] Microsoft Security Bulletin MS11-050 - Critical: Cumulative Security Update for Internet Explorer (2530548) (http://www.microsoft.com/technet/security/bulletin/ms11-050.mspx).

[*4] Microsoft Security Bulletin MS11-020 - Critical: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (http://www.microsoft.com/technet/security/bulletin/ms11-020.mspx).

[*5] Microsoft Security Bulletin MS11-026 - Important: Vulnerability in MHTML Could Allow Information Disclosure (2503658) (http://www.microsoft.com/technet/security/bulletin/ms11-026.mspx).

[*6] Microsoft Security Bulletin MS11-043 - Critical: Vulnerability in SMB Client Could Allow Remote Code Execution (2536276) (http://www.microsoft.com/technet/security/bulletin/ms11-043.mspx).

[*7] APSB11-08 Security updates available for Adobe Reader and Acrobat (http://www.adobe.com/support/security/bulletins/apsb11-08.html).

[*8] APSB11-16 Security updates available for Adobe Reader and Acrobat (http://www.adobe.com/support/security/bulletins/apsb11-16.html).

[*9] APSB11-07 Security update available for Adobe Flash Player (http://www.adobe.com/support/security/bulletins/apsb11-07.html).

[*10] APSB11-12 Security update available for Adobe Flash Player (http://www.adobe.com/support/security/bulletins/apsb11-12.html).

[*11] APSB11-13 Security update available for Adobe Flash Player (http://www.adobe.com/support/security/bulletins/apsb11-13.html).

[*12] APSB11-18 Security update available for Adobe Flash Player (http://www.adobe.com/support/security/bulletins/apsb11-18.html).

[*13] APSB11-17 Security update available for Adobe Shockwave Player (http://www.adobe.com/support/security/bulletins/apsb11-17.html).

[*14] Oracle Java SE Critical Patch Update Advisory - June 2011 (http://www.oracle.com/technetwork/topics/security/javacpujune2011-313339.html#PatchTable JAVA).

[*15] For more details on this vulnerability, see the following blog post from Context Information Security that brought it to light "WebGL - A New Dimension for Browser Exploitation" (http://www.contextis.com/resources/blog/webgl/).

[*16] About Security Update 2011-003 (http://support.apple.com/kb/HT4657).

[*17] About the security content of Mac OS X v10.6.8 and Security Update 2011-004 (http://support.apple.com/kb/HT4723).

[*18] Microsoft Security Bulletin MS11-035 - Critical: Vulnerabilities in WINS Could Allow Remote Code Execution (2524426) (http://www.microsoft.com/technet/security/bulletin/ms11-035.mspx).

[*19] APSB11-11 Security update available for Adobe Flash Media Server (http://www.adobe.com/support/security/bulletins/apsb11-11.html).

[*20] Oracle Critical Patch Update Advisory - April 2011 (http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html).

[*21] Large RRSIG RRsets and Negative Caching can crash named (http://www.isc.org/software/bind/advisories/cve-2011-1910).

[*22] Apache HTTP Server 2.2.19 Released (http://www.apache.org/dist/httpd/Announcement2.2.html).

[*23] WordPress 3.1.4 (and 3.2 Release Candidate 3) (http://wordpress.org/news/2011/06/wordpress-3-1-4/).

[*24] About the security content of iOS 4.3.2 Software Update (http://support.apple.com/kb/HT4606).

become active again*[25], and attempts to exploit SNS*[26] and Google Image Search*[27] continued to occur. Additionally, there were multiple reports of scareware downloaded in these incidents that targeted Mac OS X*[28].

Other incidents included the discovery of multiple malware targeting the Android OS smartphone platform in applications distributed through legitimate application markets*[29]. There was also a large-scale systems failure in the business system of a financial institution in South Korea that is thought to have been caused by an attack*[30]. It shut down the system for several days, severely impacting users. Additionally, law enforcement agencies in the United States shut down C&C servers and seized domains as part of an initiative to stop the activity of the Coreflood botnet, said to have infected over 2 million PCs worldwide*[31].

■ Other

Regarding trends not directly related to incidents, World IPv6 Day*[32] was held in June to test IPv6 services on a worldwide scale. ISPs in Japan also began blocking child pornography sites*[33]. Additionally, the Diet passed the “Act on the Partial Revision of the Penal Code, etc., in Response to the Sophistication of Information Processing,” which details punishment for the creation of computer viruses and other malicious code*[34].

1.3 Incident Survey

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

1.3.1 DDoS Attacks

Today, DDoS attacks on corporate servers are almost a daily occurrence, and the methods involved vary widely. 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.

■ Direct Observations

Figure 2 shows the circumstances of DDoS attacks handled by the IIJ DDoS Defense Service between April 1 and June 30, 2011. This information shows traffic anomalies judged to be attacks based on IIJ DDoS Defense Service

*25 Details on the activity of LizaMoon can be found in the following IBM Tokyo SOC Report. “A New Type of Website Alteration SQL Injection Attack (Follow-up)” (https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/sqlinjection_20110516) (in Japanese).

*26 Attacks utilizing SNS included the example detailed in the following F-Secure blog post. “Facebook Attack Spreading both Windows AND Mac malware” (http://www.f-secure.com/weblog/archives/00002172.html).

*27 Details of this incident can be found in the following F-Secure blog post. “Using Google Web Search to Find Compromised Google Images” (http://www.f-secure.com/weblog/archives/00002161.html).

*28 Details on scareware that operates on Mac OS can be found in the following Trend Micro security blog post. “More Malware Targeting Mac Users” (http://blog.trendmicro.co.jp/archives/4225) (in Japanese).

*29 Details of malware distributed over the Android Market can be found on the SOPHOS naked security blog. “Android market affected by SMS Trojans” (http://nakedsecurity.sophos.com/2011/05/13/android-market-affected-by-sms-trojans/).

*30 Details of this incident can be found in the following Network World report. “South Korea probes possible cyber attack on large bank” (http://www.networkworld.com/news/2011/041911-south-korea-probes-possible-cyberattack.html).

*31 Details of the takedown of this botnet can be found in the following joint announcement from the United States Department of Justice and the FBI. “More Than 2 Million Computers Infected with Keylogging Software as Part of Massive Fraud Scheme” (http://www.justice.gov/opa/pr/2011/April/11-crm-466.html).

*32 Details on World IPv6 Day can be found in the following document published by the Task Force on IPv4 Address Exhaustion. “World IPv6 Day Guide” (http://www.kokatsu.jp/blog/ipv4/event/W6D.pdf) (in Japanese). Official information can be found on the following page set up by the Internet Society. “World IPv6 Day” (http://www.worldipv6day.org/).

*33 Internet Content Safety Association “Initiatives to Prevent Circulation such as the Blocking of Sites Containing Images of Child Pornography Begin” (http://www.netsafety.or.jp/news/press/press-003.html) (in Japanese). See also “Internet Topics: The Blocking of Child Pornography by ISPs in Japan” for more information on these activities.

*34 Details of the bill and a FAQ can be found on the following Ministry of Justice site. “Act on the Partial Revision of the Penal Code, etc., in Response to the Sophistication of Information Processing” (http://www.moj.go.jp/keiji1/keiji12_00025.html) (in Japanese). Also see the Ministry of Justice’s comments in “Crimes Related to So-Called Computer Viruses” (http://www.moj.go.jp/content/000076666.pdf) (in Japanese).

standards. IIJ has also responded to other DDoS attacks, but these incidents are excluded from the figure due to the difficulty in accurately ascertaining the facts of each situation.

There are many methods that can be used to carry out a DDoS attack, and the capacity of the environment attacked (bandwidth and server performance) will largely determine the degree of impact. Figure 2 categorizes DDoS attacks into three types: attacks on bandwidth capacity*[35], attacks on servers*[36], 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 549 DDoS attacks. This averages to 6.0 attacks per day, indicating a decrease 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 75% of all incidents, and compound attacks accounted for the remaining 25%.

The largest attack observed during the period under study was classified as a server attack, and resulted in 131Mbps of bandwidth using up to 30,000pps packets. Of all attacks, 89% ended within 30 minutes of commencement, while 11% lasted between 30 minutes and 24 hours. No attacks continued for longer than 24 hours. The longest sustained attack was a server attack that lasted for 16 hours. 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*[37] and botnet*[38] usage as the method for conducting DDoS attacks.

Backscatter Observations

Next we present our observations of DDoS attack backscatter using the honeypots*[39] set up by the MITF, a malware activity observation project operated by IIJ*[40]. By monitoring backscatter it is possible to detect DDoS attacks occurring on external networks as a third party without any interposition. For the backscatter observed between April 1 and June 30, 2011, Figure 3 shows trends in packet numbers by port, and Figure 4 shows the sender's IP addresses classified by country.

The port most commonly targeted by the DDoS attacks observed was the 80/TCP port used for Web services, accounting for 44.5% of the total during the target period. Attacks on 3389/TCP used for remote desktop and 53/TCP

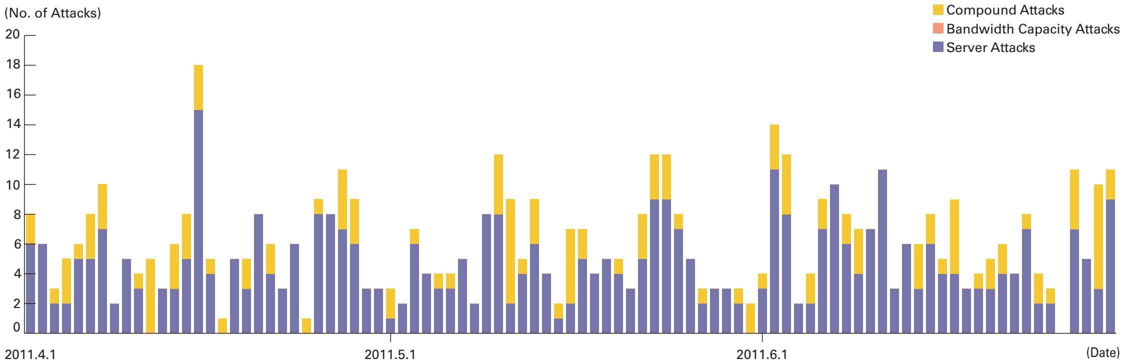


Figure 2: Trends in DDoS Attacks

[35] 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.

[36] 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.

[37] 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.

[38] 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."

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

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

used by DNS were also observed. Looking at the origin of backscatter thought to indicate IP addresses targeted by DDoS attacks by country in Figure 4, Argentina, the United States, China, and Japan accounted for large proportions at 31.6%, 25.1%, 18.5%, and 10.6%, respectively, with other countries following in order.

Following on from our previous report period, attacks on multiple ports resembling a port scan were observed on a number of IP addresses in Argentina up until May 16. A surge in DDoS attacks targeting the 80/TCP port was observed several times in May and beyond. Three of the increases in May were targeted mainly at IP addresses held by hosting companies in Japan. On May 26 a significant number of attacks on 7001/TCP were observed, but all targeted two IP addresses in China.

Multiple DDoS attacks carried out by groups such as Anonymous also became a topic of discussion during the current survey period*[41]. Of these, IIJ observations detected backscatter thought to result from attacks on Sony-related sites, attacks on sites belonging to U.S. company General Electric, and attacks on Brazilian government sites.

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the MITF*[42], a malware activity observation project operated by IIJ. The MITF uses honeypots*[43] 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.

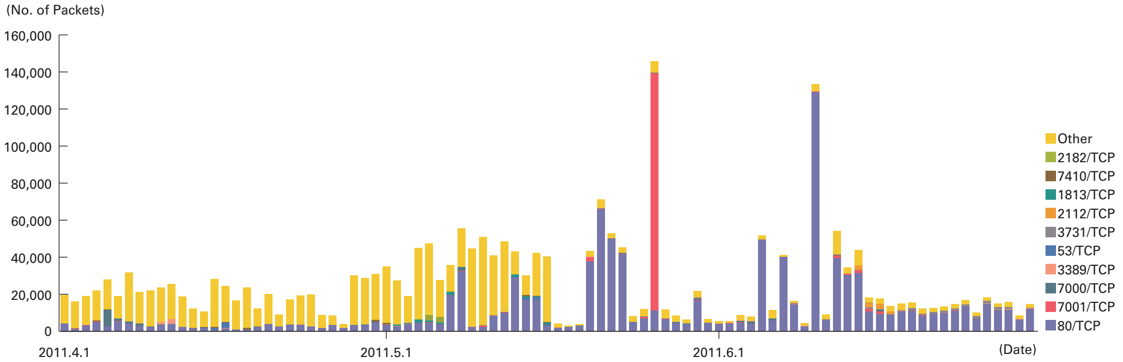


Figure 3: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)

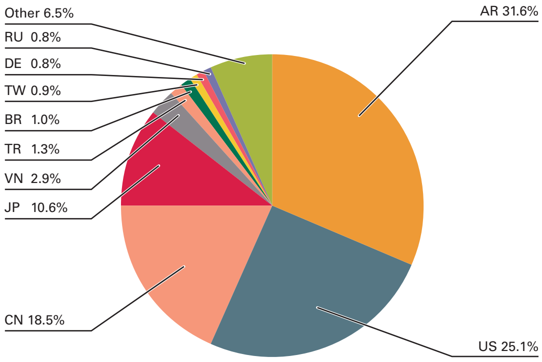


Figure 4: Distribution of DDoS Attack Targets According to Backscatter Observations (by Country, Entire Period under Study)

*41 The series of incidents carried out by groups such as Anonymous and LulzSec are explained under "1.4.1 Continuing Attacks on Companies and Government-Related Organizations."

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

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

■ Status of Random Communications

Figure 5 shows trends in the total volumes of communications coming into the honeypots (incoming packets) between April 1 and June 30, 2011. Figure 6 shows the distribution of sender's IP addresses by country. The MITF has set up numerous honeypots for the purpose of observation. We have taken the average per honeypot, showing the trends for incoming packet types (top ten) over the entire period subject to study. Additionally, in these observations we corrected data to count multiple TCP connections as a single attack when the attack involved multiple connections to a specific port, such as attacks on MSRPC.

Much of the communications arriving at the honeypots demonstrated scanning behavior targeting TCP ports utilized by Microsoft operating systems. We also observed scanning behavior for 1433/TCP used by Microsoft's SQL Server and 22/TCP used for SSH. Additionally, communications of an unknown purpose were observed on ports not used by common applications, such as 2582/TCP, 26723/TCP, and 31259/TCP. Looking at the overall sender distribution by country in Figure 6, we see that attacks sourced to China at 20.7% and Japan at 19.0% were comparatively higher than the rest.

■ Malware Network Activity

Figure 7 shows trends in the total number of malware specimens acquired during the period under study, while Figure 8 shows trends in the number of unique specimens. Figure 9 shows the distribution of the specimen acquisition source for malware. In Figure 7 and Figure 8, the trends in the number of acquired specimens show the total number of specimens acquired per day*44, while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*45. Specimens are also identified using anti-virus software, and a breakdown of the top 10 variants is displayed color coded by malware name.

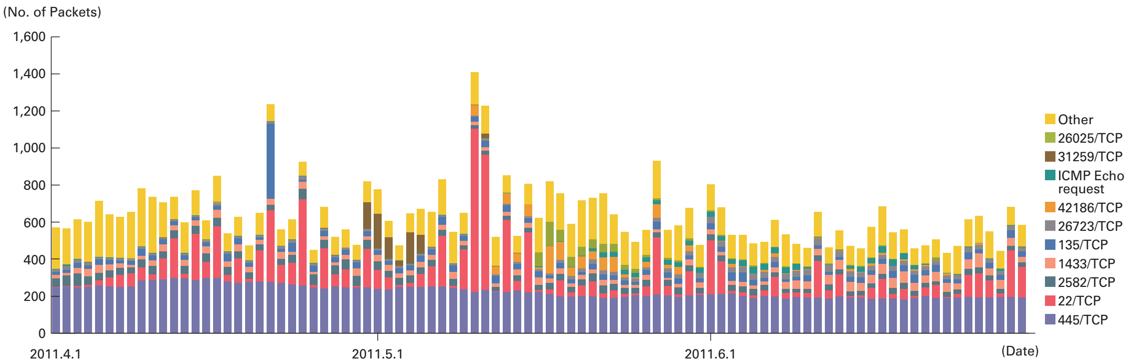


Figure 5: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

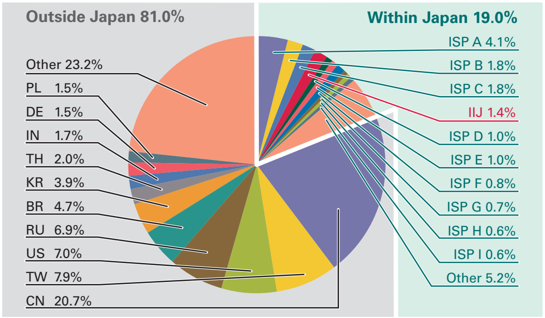


Figure 6: Sender Distribution (by Country, Entire Period under Study)

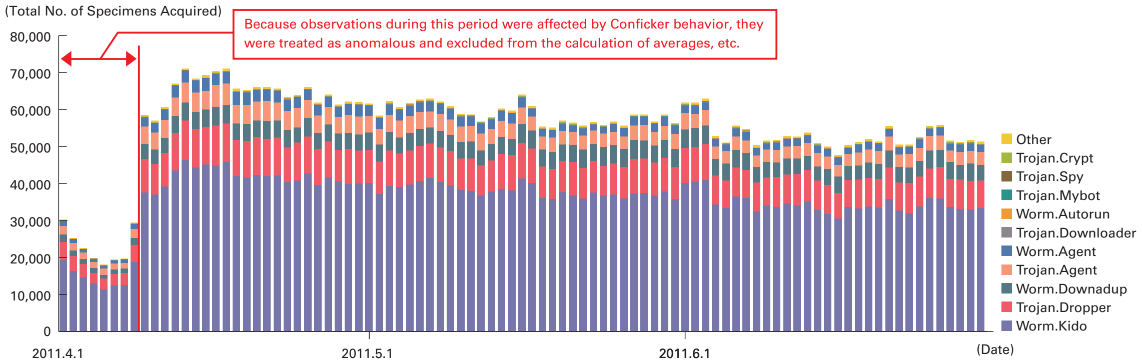
*44 This indicates the malware acquired by honeypots.

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

From this report we conducted observations using a new system based on Dionaea[*46]. Fewer specimens were acquired between April 1 and April 8 compared to the period after this. This is because a number of Conficker variants were attacking the honeypots repeatedly, placing a load on the observation system. IIJ investigated the cause of this by analyzing the Dionaea implementation, MSRPC protocol, and Conficker. As a result, we determined that this phenomenon would not abate until Conficker behavior changed. For this reason, we revised our observation system to deny access for a certain period of time from attack sources for which a specimen had already been acquired. We confirmed that this revision solved the issue of the same specimen being acquired multiple times on an infected PC, and the reduced load increased the number of other specimens acquired. We also treated observation data for the period affected by this issue as anomalous, and excluded it from the calculation of averages, etc.

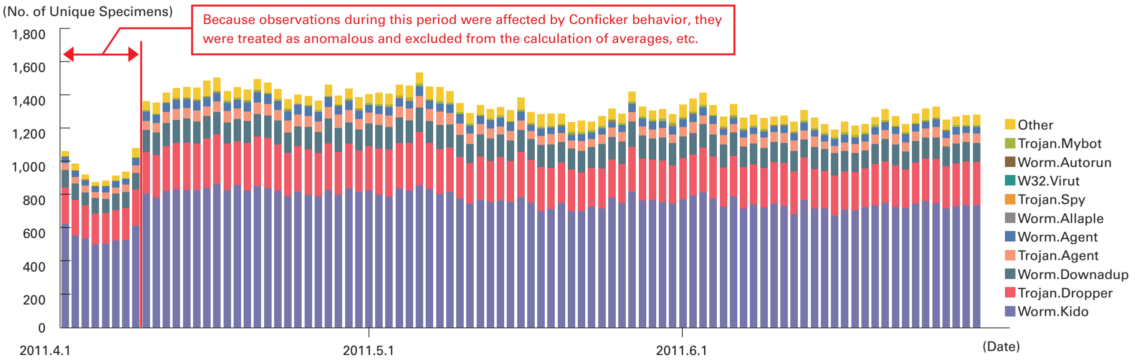
On average, 58,368 specimens were acquired per day during the period under study, representing 1,343 different malware variants. Conficker variants (Worm.Kido and Worm.Downadup in Figure 7 and Figure 8) were the dominant form of malware, accounting for 72.4% of the total number of specimens acquired, and 67.2% of unique specimens. The distribution of specimens according to source country in Figure 9 had Japan at 2.7%, with other countries accounting for the 97.3% balance. The distribution by country shows Russia at 16.0%, Taiwan at 11.7%, Brazil at 9.9%, and the United States at 9.2%. This is mainly because Conficker was active on a large-scale outside Japan.

The MITF prepares analytical environments for malware, conducting its own independent analyses of acquired specimens. During the current period under observation 75.1% of the malware specimens acquired were worms, 2.3% were bots, and 22.6% were downloaders. In addition, the MITF confirmed the presence of 23 botnet C&C servers[*47] and 17 malware distribution sites.



Because observations during this period were affected by Conficker behavior, they were treated as anomalous and excluded from the calculation of averages, etc.

Figure 7: Trends in the Number of Malware Specimens Acquired



Because observations during this period were affected by Conficker behavior, they were treated as anomalous and excluded from the calculation of averages, etc.

Figure 8: Trends in the Number of Unique Specimens

[*46] Dionaea (http://dionaea.carnivore.it/) and its functions are also explained in IIR Vol.11 (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol11.pdf) under "1.4.1 The Dionaea Honeypot".

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

1.3.3 SQL Injection Attacks

Of the types of different Web server attacks, IIJ conducts ongoing surveys related to SQL injection attacks*48. SQL injection attacks have flared up in frequency numerous times in the past. SQL injections are known to occur in one of three attack patterns: those that attempt to steal data, those that attempt to overload database servers, and those that attempt to rewrite Web content.

Figure 10 shows trends in the numbers of SQL injection attacks against Web servers detected between April 1 and June 30, 2011. Figure 11 shows the distribution of attacks according to source. These are a summary of attacks detected by signatures on the IIJ Managed IPS Service.

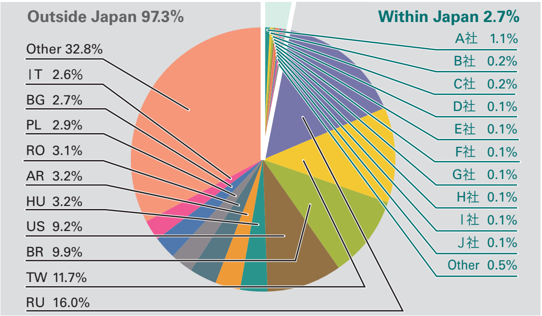


Figure 9: Distribution of Acquired Specimens by Source (by Country, Entire Period under Study)

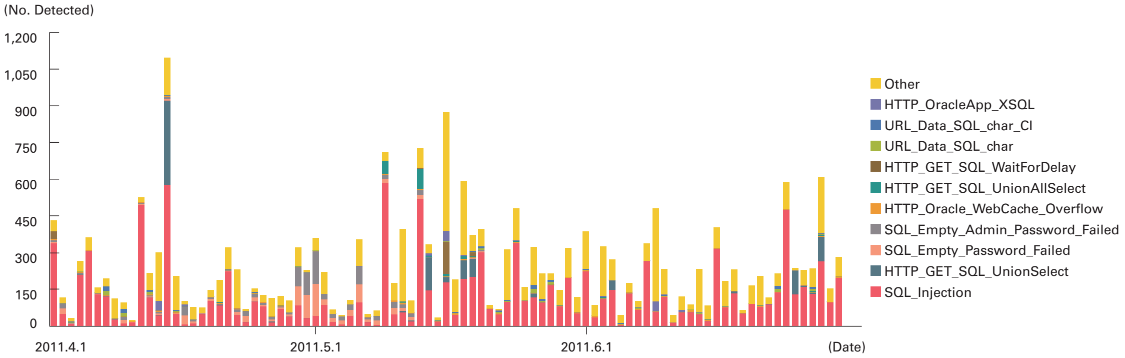


Figure 10: Trends in SQL Injection Attacks (by Day, by Attack Type)

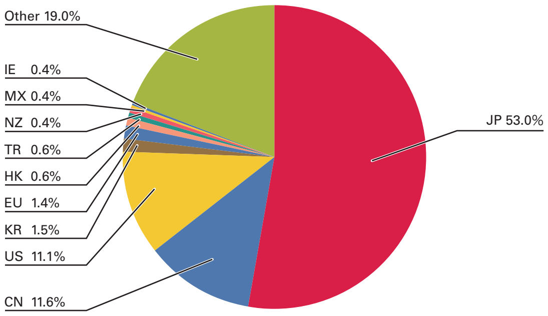


Figure 11: Distribution of Acquired Specimens by Source (by Country, Entire Period under Study)

*48 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.

Japan was the source for 53.0% of attacks observed, while China and the United States accounted for 11.6% and 11.1%, respectively, with other countries following in order. There was little change from the previous period in the number of SQL injection attacks against Web servers that occurred. The ratio of attacks from Japan and China has increased, but this is due to the decrease in attacks from the United States that were prevalent during the previous period, so there has been little change in the actual number of attacks. There were also reports that the LizaMoon malware we discussed in our previous report that alters websites using SQL injection attacks was once again active, but we could not confirm any attacks on our customer networks.

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

1.4 Focused Research

Incidents occurring over the Internet change in type and scope from one minute to the next. Accordingly, IIJ works toward implementing countermeasures by continuing to perform independent surveys and analyses of prevalent incidents. Here, we present information from the surveys we have undertaken during this period regarding a series of attacks targeting companies and government agencies that have taken place since the end of last year, and examine guidelines for dealing with issues such as DDoS attacks at telecommunications carriers.

1.4.1 Continuing Attacks on Companies and Government-Related Organizations

During the three months under study (April to June 2011), there were a large number of attacks on companies and other organizations worldwide, as well as many information leaks*[49]. During this period the movement named “Anonymous”, which had previously carried out a series of politically-motivated DDoS attacks, expanded their scope of activity and became more active*[50]*[51]. Here we recap these incidents, while analyzing changes in the nature of the attacks, and discussing steps to be taken in the future.

■ Major Topics

Table 1 shows the main security incidents that occurred during this period. A series of large-scale information leaks took place, starting with the leaking of the email addresses of several million users from marketing service Epsilon. The leak of personal information for a total of approximately 100 million users from PSN (PlayStation Network) and SOE (Sony Online Entertainment) was on a scale not seen before.

Another major topic of discussion was the many leaks carried out by LulzSec, which became active out of nowhere in May. LulzSec is said to be a group originating from Anonymous, and be comprised of the members behind the hacking of security company HBGary in February of this year. They hacked into a large number of servers, including media companies such as Fox and PBS, Sony-related companies, game developers, and sites related to the U.S. senate and FBI, and on many occasions released internal information they obtained. They directed particular focus on Sony Corporation, attacking the sites of affiliated companies at least four times. At the same time other companies around the world were also targeted, resulting in a total of at least 20 major attacks*[52].

*49 DataLossDB (http://datalossdb.org/), which records information leaks around the world, noted 90 incidents in June. This is second only to the number recorded (95 incidents) in December 2008.

*50 Anonymous is a movement said to have been conceived on an anonymous message board in the United States in around 2006. Anyone is able to participate in its activities, and the name Anonymous is also sometimes used to refer to individuals who take part. They became known to the world after protesting against a religious organization in 2008. AnonOps, which wields a great deal of influence within Anonymous, has launched DDoS attacks on a large number of sites in the name of Internet freedom, among other causes. At the end of last year they launched DDoS attacks on companies who blocked donations to WikiLeaks, such as PayPal, Visa, and MasterCard. This year, during protests seeking democracy in Tunisia and Egypt, Anonymous also launched DDoS attacks on websites related to those governments.

*51 The use of DDoS attacks, etc., to champion a political cause on the Internet is known as “hacktivism.” This is a word created from a combination of “hack” and “activism.”

*52 The following site contains details on the attacks carried out on Sony-related companies to date. Absolute Sownage (http://attrition.org/security/rants/sony_aka_sownage.html).

Table 1: List of Attacks on Companies and Government Agencies, and Information Leaks (April to June 2011)

*Bold text indicates attacks on Sony-affiliated companies, gray highlights indicate attacks linked to Anonymous, and red highlights indicate attacks linked to LulzSec and AntiSec.

Date	Overview	Type	Attacker
04.01	Marketing services firm Epsilon was hacked into and the personal information (email address) of many corporate customers leaked. The addresses of several million people are thought to have been stolen.	Information leak	
04.03	**Anonymous launched a DDoS attack on Sony. (#OpSony)**	DoS	Anonymous
04.08	Information on over 400,000 customers of major South Korean finance company Hyundai Capital was leaked.	Information leak	
04.11	The personal information of approximately 3.5 million people was leaked from a Texas state authority in the U.S.	Information leak	
04.12	Security vendor Barracuda Networks was the target of an SQL injection attack during maintenance of its WAF (Web Application Firewall), and internal information was leaked.	Information leak	
04.13	Banking operations at Nonghyup, a South Korean agricultural cooperative, were halted by the execution of a malicious program. All ATM, Internet, and over-the-counter services were frozen for several days.	DoS	
04.13	Major blog service company Wordpress.com was hacked into and administrator privileges gained.	Information leak	
04.17	The Oak Ridge National Laboratory that is affiliated with the United States Department of Energy was the subject of a targeted attack via email.	Targeted attack	
04.20	Anonymous launched DDoS attacks on major Italian power company ENEL and major French power company EDF. (#OperationGreenRights)	DoS	Anonymous
04.26	Anonymous began a DDoS attack on the New Zealand government. (#OpNZBlackOut)	DoS	Anonymous
04.26	**The personal information of approximately 77 million PlayStation Network (PSN) users was leaked.**	Information leak	
05.01	Anonymous began a DDoS attack on the Iran government. (#OpIran)	DoS	Anonymous
05.02	**The personal information of approximately 26.4 million Sony Online Entertainment (SOE) users was leaked.**	Information leak	
05.05	Major password management service LastPass was hacked into, and it is possible that user and password information was leaked.	Information leak	
05.05	**The Sony Music Greece website was partially altered. Personal information was also leaked.**	Information leak, alteration	
05.06	**Some personal information from U.S. Sony Electronics was leaked.**	Information leak	
05.07	LulzSec published information on applicants for the U.S. audition show X Factor.	Information leak	LulzSec
05.10	LulzSec hacked into major U.S. television network Fox and released internal information.	Information leak	LulzSec
05.11	**The Sony Music Indonesia website was partially altered.**	Alteration	
05.14	Personal information from the European subsidiary of Square Enix was leaked.	Information leak	Anonymous
05.15	Anonymous launched another DDoS attack on ENEL. (#OperationGreenRights)	DoS	Anonymous
05.16	At Japanese Internet service provider So-net, a Sony-affiliated company, an attacker used another person's redeemable gift points without authorization.	Account theft	
05.19	The personal information of approximately 5,200 users of the game point service gamer-point.net was leaked.	Information leak	
05.20	**The Sony Thailand website was partially altered and a phishing site was run under this site.**	Alteration	
05.22	Anonymous launched another DDoS attack on ENEL. (#OperationGreenRights)	DoS	Anonymous
05.23	Security service company Comodo Brazil was the target of an SQL injection attack, and internal information was leaked.	Information leak	
05.24	Anonymous launched a DDoS attack on U.S. Chamber of Commerce site uschamber.com. (#Operation Payback)	DoS	Anonymous
05.24	**The Sony Ericsson Canada website was the target of an SQL injection attack perpetrated by Lebanese hacker Idahc, and the personal information of approximately 2,000 users was leaked.**	Information leak	Idahc
05.24	**An SQL injection vulnerability was discovered in the Sony Pictures Italia website.**	Information leak	
05.24	**An SQL injection vulnerability was discovered in the Sony Music Entertainment (Japan) website.**	Information leak	LulzSec
05.27	Major U.S. aerospace/defense contractor Lockheed Martin was hacked into. No information was leaked due to their quick response. SecurID information leaked from RSA in March was exploited.	Targeted attack	
05.27	It was revealed that information on approximately 283,000 customers of Honda Canada was leaked in February.	Information leak	
05.28	There was unauthorized access at the online shop of furniture retailer Unico. The personal information of approximately 17,000 individuals was leaked.	Information leak	
05.30	Public Broadcasting Service (PBS) was hacked by LulzSec. Fake articles were posted on its news site, and a large volume of internal personal information including email addresses and passwords was leaked.	Information leak, alteration	LulzSec
06.02	Google reported that Gmail mail accounts had been used without authorization. This affected several hundred people, including U.S. government officials and Chinese activists. User names and passwords were obtained through phishing, and settings changed to forward all mail to an external account.	Targeted attack	
06.03	Anonymous released classified documents (including emails regarding the issue of visas) from the Iranian Ministry of Foreign Affairs. (#OpIran)	Information leak	Anonymous
06.03	Anonymous launched another DDoS attack on EDF. (#OperationGreenRights)	DoS	Anonymous
06.03	Security company Trend Micro reported that attacks similar to those on Gmail had also been made on Hotmail and Yahoo! Mail.	Targeted attack	
06.03	**LulzSec leaked information from U.S. Sony Pictures, Sony BMG Belgium, and Sony BMG Netherlands. Sony Pictures later admitted that information on approximately 37,500 customers was leaked.**	Information leak	LulzSec
06.04	LulzSec hacked the website of Infragard Atlanta and released the personal information of approximately 180 people. They also released approximately 1,000 emails from Infragard partner Unveillance. Infragard is a non-profit organization jointly operated by the FBI and private U.S. businesses that carries out information sharing and analysis.	Information leak	LulzSec
06.04	Part of the server configuration files for U.S. Nintendo.com were released by LulzSec. Nintendo commented that they were hacked a few weeks earlier, but did not announce the fact as no personal information was included.	Information leak	LulzSec
06.04	The European site for major Taiwanese PC manufacturer Acer was hacked by the PCA (Pakistan Cyber Army), and the personal information of over 40,000 individuals was leaked.	Information leak	PCA
06.04	**Sony Europe was hacked by Lebanese hacker Idahc, and the personal information of 120 individuals was leaked.**	Information leak	Idahc

Date	Overview	Type	Attacker
06.05	**An SQL injection vulnerability was revealed in the Sony Pictures Russia website. No personal information was leaked.**	Information leak	
06.05	**It was discovered that the Sony Music Brazil website had been altered since November of last year.**	Alteration	
06.06	The source code for Sony Computer Entertainment's Developer Network (scedev.net) and Sony BMG's internal network information were released by LulzSec.	Information leak	LulzSec
06.08	It was announced that unauthorized access had taken place at the GEO E Shop in April, and customer information was leaked.	Information leak	
06.08	**There was unauthorized use of accounts by an attacker at Sony Points. 95 email addresses were used to exchange 27,800 points (worth approximately 280,000 yen) without authorization.**	Account theft	
06.09	U.S. Citigroup was hacked and information leaked. The credit card information of approximately 360,000 customers with Citi Cards was leaked, incurring damages of about 2.7 million dollars.	Information leak	
06.09	**Sony Music Portugal (sonymusic.pt) was hacked by Idahc, and the email addresses of approximately 350 users leaked.**	Information leak	Idahc
06.10	Anonymous launched a DDoS attack on major U.S. agricultural bioscience manufacturer Monsanto. (#OperationGreenRights)	DoS	Anonymous
06.10	U.K. game developer Codemasters was hacked, and customer information leaked.	Information leak	
06.10	A dispute between China and Vietnam revolving around territorial rights in the South China Sea escalated. There was an increase in cyber attacks, and over 1,500 sites in Vietnam were altered.	Alteration	
06.12	It was reported that the International Monetary Fund (IMF) had been targeted in a large-scale attack.	Targeted attack	
06.12	**SQL injection vulnerabilities in three Sony-related sites were made public by LulzSec. No personal information was leaked.**	Information leak	LulzSec
06.13	Unauthorized access took place at game developer Epic Games, and the company was forced to reset user passwords.	Information leak	
06.14	LulzSec hacked into game company Bethesda and U.S. Senate site Senate.gov and released information they obtained.	Information leak	LulzSec
06.15	LulzSec launched DDoS attacks on a number of game-related sites.	DoS	LulzSec
06.16	Anonymous launched DDoS attacks on sites related to the Malaysian government. At least 41 sites were affected.	DoS	Anonymous
06.16	LulzSec launched DDoS attacks on a number of sites. Targets were selected randomly by soliciting phone requests. The CIA was attacked last, bringing its site down temporarily.	DoS	LulzSec
06.17	Anonymous launched DDoS attacks on sites related to the Spanish, Syrian, and Turkish governments.	DoS	Anonymous
06.17	Game developer BioWare was hacked. The personal information of 18,000 individuals was leaked.	Information leak	
06.18	The SEGAPASS service operated by SEGA's European subsidiary was hacked. The personal information of approximately 1.3 million individuals was leaked.	Information leak	
06.19	Anonymous launched a DDoS attack on U.S. company GE (www.ge.com). (#OperationGreenRights)	DoS	Anonymous
06.20	Account information was leaked from the Mt. Gox site for exchanging the Bitcoin virtual currency. The Bitcoin exchange rate plummeted temporarily after this account information was used in unauthorized transactions.	Account theft Information leak	
06.20	**Idahc and other hackers discovered an SQL injection vulnerability in the Sony Pictures France website, and some information was made public.**	Information leak	Idahc
06.20	Domain registration company Network Solutions was targeted in DDoS attacks on 6/20 and 6/21.	DoS	
06.21	It was discovered that the StartCom certificate authority service was hacked on 6/15. There was no impact on the issuing of certificates.	Information leak	
06.23	Customer information was leaked from U.S. mobile communications operator Virgin Mobile.	Information leak	AntiSec
06.24	LulzSec released internal information from an Arizona state authority in the U.S.	Information leak	AntiSec
06.24	Anonymous launched a DDoS attack on major German pharmaceutical company Bayer. (#OperationGreenRights)	DoS	Anonymous
06.25	Anonymous launched a DDoS attack on sites related to the Brazilian government. (#OpBrazil)	DoS	Anonymous
06.25	The hacker team TeaMp0isoN released the personal information (webmail address book) of former U.K. prime minister Tony Blair.	Information leak	TeaMp0isoN
06.27	Anonymous attacked and altered sites related to the Tunisian government.	Alteration	Anonymous
06.29	LulzSec released another set of internal information from an agency in the U.S. state of Arizona.	Information leak	AntiSec
06.29	Internal information was leaked from U.S. media group company Viacom and major record company Universal Music.	Information leak	AntiSec
06.29	Anonymous launched a DDoS attack on a site belonging to a municipal authority in the U.S. city of Orlando, Florida. (#OpOrlando)	DoS	Anonymous
06.29	A DDoS attack was launched on U.S. message board site 4chan.org.	DoS	
06.29	A DDoS attack was launched on MasterCard. MasterCard denied the attack, however, saying there was a problem with their ISP.	DoS	
06.29	The authentication information of a number of MySpace and PayPal users was leaked.	Information leak	
06.30	The personal information of approximately 300,000 users was leaked from an Indian subsidiary of Groupon (SoSasta). The entire contents of their database were searchable using Google.	Information leak	

(Note 1) Operation Anti-Security (AntiSec) was a cooperative effort between LulzSec and Anonymous that began on June 20, and attacks involved a range of participants and sources, but here it is classified as a LulzSec attack because they were the initiators.

(Note 2) All the incidents mentioned in this table are based on information that was made available to the general public on news sites, etc.

Anonymous also launched DDoS attacks on Sony Corporation, power companies in Italy and France, and government-related sites in New Zealand, Iran, the United States, Malaysia, Syria, Spain, Turkey, and Brazil. Attacks around the world escalated after LulzSec announced they would carry out Operation Anti-Security (AntiSec) together with Anonymous in late June*[53]. 50 days after their first attack, LulzSec suddenly declared they would cease their activities*[54]. However, AntiSec attacks by Anonymous have not abated, and continue with a growing number of participants.

Other noteworthy incidents include a series of targeted attacks on organizations related to U.S. national defense*[55]. Organizations affiliated with the U.S. Department of Energy such as Oak Ridge National Laboratory were the first attacked, forcing the network to be isolated from external access while services were restored. Lockheed Martin was also attacked through the exploitation of information that was leaked from RSA (EMC) in March of this year*[56]. Other companies involved with national defense such as L-3 Communications and Northrop Grumman were also attacked during the same period. This may have been a series of attacks aimed at stealing military secrets, but the details are not known.

■ Analysis

The most high-profile activities during the current survey period were incidents carried out by Anonymous, LulzSec, and AntiSec. Here we will analyze these attacks in more detail.

■ Developments in the Attack Activities

Anonymous is sometimes referred to as a "hacker group" in the media. However, rather than being a group comprised of specific members, Anonymous is an extremely loose-knit collective of individuals who share a common world view. There is no set leader or core organization. This begs the question of how the target of each attack is decided. The key point here is the activities and transmission of information in each region. Anonymous is active throughout the world. However, is it not regulated as a single entity, with activities being carried out independently in each region at the same time. For example, when Internet censorship is uncovered in a certain region, individuals in that region begin to speak out against it, sending information over the Internet. At the same time Anonymous in that region decide on a target to attack, determine details such as the timing, and call on other supporters for help*[57]. Members of Anonymous around the world answer this call, and participate in DDoS attacks. Meanwhile, LulzSec is a team comprised of a small number of members who employ methods completely different to those used by Anonymous*[58].

■ Attack Target Selection

Two types of target selection were observed. The first type was indiscriminate attacks. These attacks begin without warning, either for no particular reason, or for a reason that was tailored to the situation later. For example, a site with a vulnerability is first found using a search engine like Google. It is then attacked, and internal information obtained illegally is released. The DDoS attacks LulzSec carried out towards the end of its period of activity by soliciting phone requests could be categorized as typical indiscriminate attacks. While LulzSec carried out attacks with political objectives in the same way as Anonymous, they also launched attacks purely for entertainment value (described as "for the lulz"). From the perspective of those defending against such attacks, they are hard to anticipate and it is easy to be caught off guard.

The second pattern observed was persistent attacks on a specific target. As mentioned previously, over 20 attacks on Sony-affiliated companies took place around the world, but these activities were not coordinated together*[59]. At the same time, attacks were made on other companies in the games industry, with several game-related companies suffering information leaks and other damages. We can surmise that this was a series of opportunistic attacks originating from Anonymous DDoS attacks on Sony that later spread to other companies. This behavior strongly

*[53] LulzSec announcement regarding #AntiSec (http://pastebin.com/9KyA0E5v).

*[54] Announcement regarding "50 Days of Lulz" (http://pastebin.com/1znEGmHa).

*[55] See IIR Vol.7 "1.4.2 Targeted Attacks and Operation Aurora" for more information on targeted attacks (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol07_EN.pdf).

*[56] EMC mentions the attack on Lockheed Martin in an open letter to customers dated June 6 (http://www.rsa.com/node.aspx?id=3891).

*[57] Based on our observations of a number of Anonymous attacks, the details of each attack are determined through discussion or by vote. However, they do not follow a set procedure, and sometimes change suddenly partway.

*[58] According to details announced by LulzSec themselves on Twitter, etc., they are comprised of six core members.

*[59] Of more than 20 attacks, Lebanese hacker Idahc and LulzSec have each indicated they were involved in 4. The parties responsible for most of the other attacks are not known, and their connection with Anonymous and LulzSec is unclear.

resembles the “hive mind” activity often seen on message boards in Japan and the United States. Any organization could potentially bear the brunt of attacks like this.

■ Attack Motives

The difficulty of identifying motives for these attacks is another point of note. When the credit card information of 360,000 individuals was leaked from U.S. financial institution Citigroup, the leaked card information was used to commit approximately 2.7 million dollars worth of credit card fraud*[60]. It is clear that attacks like these are cyber crimes committed for financial gain. There are also many cases of websites being attacked and altered in relation to territorial disputes between nations that have reached a flash point such as India and Pakistan, and China and Vietnam. There has been similar trouble between Japan and neighboring nations in the past. These attacks involve national disputes that spill over to the Internet, and the motives behind them are easy to discern.

The recent series of attacks carried out by Anonymous and other groups are clearly of a different nature to these incidents in many cases. Specifically, there were cases where the internal information of certain organizations was obtained illegally for reasons other than exploiting it. In a number of cases the information obtained was not exploited directly, with the party responsible simply announcing what they had obtained and releasing it on the Internet. For example, LulzSec released a large amount of information it had obtained illegally, but it is thought that in most cases they did not exploit that information themselves. During the AntiSec attacks that followed, internal information that had been illegally obtained was also released on file sharing sites like MediaFire or through BitTorrent*[61], and announcements were made using Pastebin*[62], etc., but in almost all cases the attacker did not exploit this information themselves.

Although the attackers did not exploit what they obtained, when such information is released to the public it will of course be exploited by other parties. Even if it is not exploited, the party who was attacked must explain to users that information was leaked, and respond by resetting passwords, etc. The mere fact that information was leaked also unavoidably has a negative effect on the organization’s brand image and stock value. The motives behind this series of attacks may differ from other incidents, but the fact that targets suffer as a result remains unchanged.

In the past Anonymous have carried out DDoS attacks in strong opposition to actions such as censorship that inhibit the free use of the Internet. However, the activities of LulzSec and AntiSec have deviated from this goal somewhat, and it appears that their focus is shifting to use of the methods themselves such as DDoS attacks and hacking. Whether this is a temporary trend or a move towards an expanded scope of activity is not yet clear.

■ Disclosure of Attack Activities

One characteristic of the activities of Anonymous and LulzSec is they have disclosed the majority of their attacks. Anonymous attacks are coordinated over IRC channels. Most of these are open channels that anyone can join*[63]. They also actively share information over SNS such as Twitter and Facebook, as well as blogs. LulzSec communicates with other parties over IRC, and even organized a special channel for the media. This kind of disclosure brought them much attention and made it easier to rally supporters to their cause, while also demonstrating they had nothing to hide with regard to their activities.

■ Attack Tools

The attack methods used by Anonymous are not all that different from other attackers. Some members are familiar with advanced attack techniques, but this is not true of the majority of participants. For this reason, they developed and distribute a dedicated tool for DDoS attacks called LOIC (Low Orbit Ion Cannon)*[64]. By selecting a TCP, UDP, or HTTP protocol and entering the details of the target, a large volume of packets and connections are directed at the target. This tool can be used easily even by participants with no technical ability. In addition to a manual attack mode,

*60 “Updated Information on Recent Compromise to Citi Account Online For Our Customers” (http://www.citigroup.com/citi/press/2011/110610c.htm).

*61 A protocol for transferring (sharing) files over a P2P network, as well as software for using this network.

*62 A site that allows text to be published online anonymously (http://pastebin.com/). There are also many similar sites, such as Pastie (http://pastie.org/) and PasteHTML (http://pastehtml.com/).

*63 Anonymous operates multiple IRC servers. e.g. irc.anonops.li, etc.

*64 LOIC is available to the general public, and can be obtained by anyone.

it also features a function known as IRC mode. In this mode a user only has to enter an IRC server and channel name to connect, with attacks then carried out via remote control according to commands sent from the IRC server. This resembles the control of a botnet via commands sent from a C&C server. This means that when using LOIC's IRC mode participants voluntarily become part of a botnet.

However, LOIC has no function for spoofing the sender's IP address. This is related to the fact that Anonymous asserts that DDoS attacks are a legitimate form of protest. However, regardless of this assertion, in a number of countries obstructing services by sending large volumes of packets or initiating many connections is unlawful behavior. For this reason participants in the DDoS attacks are often arrested, and many arrests of minors have taken place*[65].

LOIC is not the only tool used in actual Anonymous DDoS attacks, as other botnets are also employed. A member of Anonymous arrested in the United Kingdom in May stated in an interview that they used a botnet under their control for DDoS attacks on Sony*[66]. IIJ's MITF malware activity observation project observed data including backscatter from multiple DDoS attacks on targets such as Sony and Brazilian government sites. Backscatter is observed when an attack spoofing the sender's IP address is carried out. Consequently, attack tools with an address spoofing function must have been used in these attacks in addition to LOIC.

■ Response

Next, we will examine what response should be taken in the future by those in the position of defending against this kind of attack. Based on analysis of the above, we will categorize responses into the following three groups based on the likelihood of being targeted.

1. Not a likely target, but may be targeted in an indiscriminate attack.
2. Falls within the targeted scope of a particular attack.
3. Already the target of attacks, or is currently being attacked.

Regarding the first category, a computer connected the Internet has the potential to be targeted in an indiscriminate attack at any time. It is therefore important to be prepared for attacks and have security measures in place so you can respond whenever an attack occurs. This involves implementing existing security measures such as the patching of vulnerabilities in servers and web applications that can be accessed externally, the configuration of boundaries using a firewall or IPS, etc., and the installation of anti-virus software. Attackers that disclose their activities like Anonymous are rare, and most attacks occur without warning. It is difficult to predict attacks in advance in this case, so the only option is to prepare as you would for an indiscriminate attack. These preparations are necessary so you can swiftly determine that an attack has occurred, and take appropriate actions based on the details of the attack and the damages incurred.

When the second category applies, countermeasures are extremely important. Taking appropriate measures when you are aware that your organization will be attacked in advance can reduce the impact of the attack or even prevent it from occurring. Specific organizations may be targeted in an attack for a variety of reasons. These include cases where your organization itself is the focus of an attack, cases where attacks spill over from another company in the same field, and cases where organizations are targeted based on certain common attributes, such as those based in Japan. This means it is a good idea to take note of information about attacks on other companies in the same field or criticism of the work of your company that is available to the general public via news articles or SNS, etc. Looking at the attacks presented in this report we can see that while Anonymous frequently uses DDoS attacks, many of the activities carried out by LulzSec and subsequently AntiSec involve information leaks via the hacking of sites using SQL injection attacks. By analyzing past and current attacks in this way it is possible to gain an understanding of the attackers and the attack methods used, predict future attacks, and use this information when implementing countermeasures. By learning that your organization may be targeted in these attacks at the earliest stage possible,

*65 Three suspects were arrested in Spain in June. Announcement by Spanish law enforcement authorities (http://www.policia.es/prensa/20110610_2.html) (in Spanish).

*66 "The fighting continues as AnonOps stages a comeback" (http://www.thetechherald.com/article.php/201119/7163/The-fightingcontinues-as-AnonOps-stages-a-comeback).

and revising server configurations and confirming software versions, it is more likely that you will be able to avoid actual damages when an attack occurs[67].

When you anticipate an attack on your organization, it is necessary to bolster your security so that attacks can be detected and dealt with as quickly as possible.

Last of all, those who fall into the third category are already aware that they are a target, or have already been attacked. When you know you will be targeted by an attack, you must find out more about the attacker, in particular their background and the reason for the attack, as well as the type of attacks they have carried out in the past. There are many reasons for attacks, ranging from the activities of your organization being brought into question to careless remarks that were made by its management. However, provided the reason is known it may be possible to avoid an attack by rectifying the problem.

By understanding the attacker's motives it is also possible to predict to a certain extent whether the attack will be a one-off incident or will continue until a goal is attained, as well as what the type and nature of the attack might be, and whether it will undergo changes in the future. For example, the series of SQL injection attacks detailed in this report have recently stopped short of resulting in information leaks, consisting of confirmation that an SQL injection vulnerability exists, and public announcement of this fact. In these cases it is believed the attacker is not launching an attack to steal information, but rather to damage the reputation of the target by announcing the existence of a vulnerability.

If an attack has already taken place, it is first important to accurately gauge its impact. You must ascertain whether customers have been affected by the service outage, whether information has been leaked, and what the details and scale of such an information leak are, and then respond based on an assessment of the impact. If attacks are still ongoing, steps must be taken to put an end to them. For example, some DDoS attacks last anywhere from several hours to several days. When your organization is unable to defend itself against an attack, it is necessary to cooperate with external organizations such as your provider, and in this case it is essential to work on building a good collaborative relationship with them on a regular basis.

After an attack occurs, you will need to disclose information appropriately in addition to restoring systems to operation, and taking steps to prevent reoccurrence. In particular, if third parties such as customers are affected, they will expect swift and accurate disclosure of the events that have taken place, and it is necessary to indicate your responsibility with regard to the events as a company or organization.

Looking at recent trends in attacks, we expect that attacks on companies and government organizations will continue to occur frequently. As indicated here, it is important that those responsible for defending against such attacks stay aware of the possibility that they may become a target, and remain adequately informed about attackers.

1.4.2 Guidelines for Dealing with Cyber Attacks Involving High Volume Communications and Secrecy of Communications at Telecommunications Carriers (Second Edition)

As shown in the previous section of this report, attacks on companies and government-related organizations are currently on the rise. Attacks can be dealt with in a number of ways depending on the methods used, but DDoS attacks in particular involve high volumes of communications and cannot be handled by the target organization alone, requiring some kind of intervention by telecommunications carriers including ISPs such as IIJ. Meanwhile, countermeasures such as the blocking of communications by providers may unavoidably encroach upon various rights of those carrying out communications. In light of this, the actions telecommunications carriers can take in response to attack communications were examined taking into consideration the protection of the secrecy of communications in accordance with the Telecommunications Business Law, and guidelines presenting examples[68] were published on March 25, 2011.

[67] For example, in the attacks on Sony it was possible to predict in advance the possibility of attacks spilling over to other Sony group companies and the game industry.

[68] The entire text of the Second Edition of these guidelines can be obtained from the following organization. Council for Stable Operation of the Internet (http://www.jaipa.or.jp/other/mtcs/index.html) (in Japanese). The following is a press release regarding the publication of guidelines from the Japan Internet Providers Association (JAIPA), which is a member of the council. "Regarding Revision of the Guidelines for Dealing with High Volume Communications and Privacy at Telecommunications Carriers" (http://www.jaipa.or.jp/other/mtcs/info_110325.html) (in Japanese).

These guidelines discuss responses to a number of types of communications thought to occur due to attacks, and at this point it is the only set of guidelines in Japan with information on how to respond to DDoS attacks. Here we discuss the information in these guidelines, with a focus on ISP responses to DDoS attacks.

■ Background to the Development of these Guidelines

These guidelines are the result of evaluating ISP responses to attacks in a variety of situations. They are based on extensive evaluation of responses to a variety of attacks involving high volumes of communications by a number of ISPs in Japan who are members of organizations such as Telecom-ISAC Japan*69. These evaluations stem from problems identified through the experience of dealing with a series of simultaneous DDoS attacks on multiple Web servers in Japan in 2005. This material was first established with the goal of publishing a collection of examples, but in 2006 communications-related organizations began work on developing them into a set of guidelines. As a result the first edition of the guidelines*70 we have today was established on May 30 2007, presenting questions, explanations, and examples in that order. Efforts to revise the guidelines began in April 2010*71 in response to escalating attacks over the Internet and a number of new attack methods that had emerged. They were released to the public in March of this year.

■ Guideline Overview and Applications

The guidelines established through the above process are targeted at issues such as DoS and DDoS cyber attacks, the spread of malware infections, the mass sending of spam emails, and irregular packets. They examine whether or not responses to these high volume communications taken by telecommunications carriers interfere with the secrecy of communications. Various scenarios involving high volume communications are discussed, presenting examples with a focus on the concept of situations where countermeasures are legally justifiable. Consequently, these guidelines do not cover responses to attacks not involving a conspicuously high volume of communications, such as measures to counteract harmful material or phishing or other legal issues such as non-discrimination, equal opportunities, or the protection of personal information, so these require separate evaluation.

Additionally, because these guidelines were drawn up independently by private industry organizations (as voluntary standards), they do not serve to absolve those who implement countermeasures in accordance with them of all responsibility. It is difficult to establish universal quantitative criteria for what to consider high volume communications because this differs depending on a provider's network structure as well as the attack methods used, so when dealing with examples of actual attacks it is considered necessary to implement measures after determining whether or not these guidelines apply to that case on an individual basis (Chapter 1, Article 2 of these guidelines). At the same time, because the status of the Internet and attacks that occur over it can change day by day, the guidelines themselves will not stay relevant forever, and it is stated within that they should be revised as necessary in light of the developing situation (Article 5).

■ Dealing with Attack Communications while Maintaining Secrecy

If an ISP notices a user is being targeted in a DDoS attack and takes measures without the user's consent such as examining the details of the attack, blocking attack communications, or sharing the information with other ISPs to ask for cooperation, it is illegal for that ISP to comply with these actions unilaterally because they all infringe upon the secrecy of communications (knowledge, use without permission, and disclosure). However, from a practical standpoint it is not possible to reduce the impact of attacks unless some or all of these measures are implemented. In this case, we must consider the conditions under which countermeasures be implemented without committing an illegal act. These guidelines provide perspective on this in Article 2 and Article 4.

First, assuming the control (including knowledge) of communications always infringes upon the secrecy of communications, cases in which this illegal action is justified include when the communicating party gives

*69 Telecom Information Sharing and Analysis Center Japan (https://www.telecom-isac.jp/english/index.html). It is also known as Telecom ISAC Japan.

*70 The following is a press release from JAIPA regarding establishment of the first edition (http://www.jaipa.or.jp/info/2007/info_070530.html) (in Japanese). For this first edition only the purpose of the text and the preface providing a general overview were released to the public, with other details only released to telecommunications carriers (companies that were members of the four participating associations).

*71 The Telecom Information Sharing and Analysis Center Japan joined members of the council responsible for the first edition to form the Council for Stable Operation of the Internet, which was responsible for evaluating the second edition.

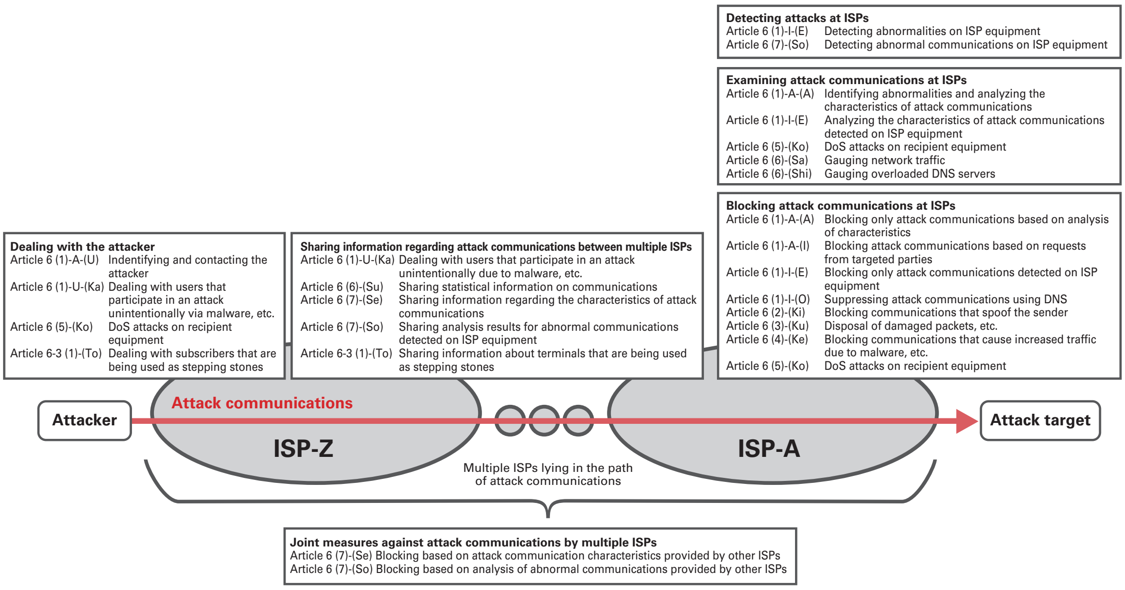
permission, when the ISP itself is the communicating party, and when such action corresponds to acts decreed by law, legitimate business operations, legitimate self-defense, or emergency measures*[72].

Here, we will look at actions that correspond to legitimate business operations. The legitimate business operations of a telecommunications operator entail those actions necessary to maintain and continue the operation of telecommunications business. The control of communications to deal with an attack is only considered justified if it constitutes a legitimate goal, is deemed necessary action, and uses appropriate methods. For example, the routers that form the Internet are devices that reference the headers in IP packets and match them with routing information to determine the destination, but referencing headers infringes upon the secrecy of communications. That said, the purpose of this action is to establish communications, and without it communications cannot take place, so because there is no method for determining the destination of IP packets other than referencing the headers, this can be treated as a legitimate business operation of telecommunications carriers. Other examples of measures required for the stable operation of networks include dealing with attacks on networks that use a high volume of communications, anti-spam measures via OP25B and IP25B, and bandwidth control.

■ Examples Presented in the Guidelines

Each section in Chapter 2 includes discussion of responses to take and the secrecy of communications under specific circumstances. A variety of attacks are examined, but here we will present information from the guidelines using DDoS attack countermeasures as an example. The information in the guidelines that covers DDoS attack countermeasures is summarized in Figure 12 under the various steps involved in dealing with DDoS, namely detecting an attack, examining an attack, blocking an attack, sharing information, dealing with the attacker, and implementing joint measures. The conditions for specific attacks and countermeasures are looked at methodically in the guidelines, so it is necessary to refer to the guidelines to determine whether or not they actually apply.

For example, in Article 6 (1)-A, "When the targeted party issues a request," while section (I) states that "examining the characteristics of attack communications and automatically blocking only communications that match the characteristics constitutes infringement of the secrecy of communications," it indicates that such action is legally justified if the communicating party consents, or "if it is carried out using reasonable methods within the scope necessary to prevent the impairment of all subscriber terminals through unauthorized attack communications." It



Detecting attacks at ISPs

Article 6 (1)-I-(E)	Detecting abnormalities on ISP equipment
Article 6 (7)-(So)	Detecting abnormal communications on ISP equipment

Examining attack communications at ISPs

Article 6 (1)-A-(A)	Identifying abnormalities and analyzing the characteristics of attack communications
Article 6 (1)-I-(E)	Analyzing the characteristics of attack communications detected on ISP equipment
Article 6 (5)-(Ko)	DoS attacks on recipient equipment
Article 6 (6)-(Sa)	Gauging network traffic
Article 6 (6)-(Shi)	Gauging overloaded DNS servers

Blocking attack communications at ISPs

Article 6 (1)-A-(A)	Blocking only attack communications based on analysis of characteristics
Article 6 (1)-A-(I)	Blocking attack communications based on requests from targeted parties
Article 6 (1)-I-(E)	Blocking only attack communications detected on ISP equipment
Article 6 (1)-I-(O)	Suppressing attack communications using DNS
Article 6 (2)-(Ki)	Blocking communications that spoof the sender
Article 6 (3)-(Ku)	Disposal of damaged packets, etc.
Article 6 (4)-(Ke)	Blocking communications that cause increased traffic due to malware, etc.
Article 6 (5)-(Ko)	DoS attacks on recipient equipment

Dealing with the attacker

Article 6 (1)-A-(U)	Indentifying and contacting the attacker
Article 6 (1)-U-(Ka)	Dealing with users that participate in an attack unintentionally via malware, etc.
Article 6 (5)-(Ko)	DoS attacks on recipient equipment
Article 6-3 (1)-(To)	Dealing with subscribers that are being used as stepping stones

Sharing information regarding attack communications between multiple ISPs

Article 6 (1)-U-(Ka)	Dealing with users that participate in an attack unintentionally due to malware, etc.
Article 6 (6)-(Su)	Sharing statistical information on communications
Article 6 (7)-(Se)	Sharing information regarding the characteristics of attack communications
Article 6 (7)-(So)	Sharing analysis results for abnormal communications detected on ISP equipment
Article 6-3 (1)-(To)	Sharing information about terminals that are being used as stepping stones

Joint measures against attack communications by multiple ISPs

Article 6 (7)-(Se)	Blocking based on attack communication characteristics provided by other ISPs
Article 6 (7)-(So)	Blocking based on analysis of abnormal communications provided by other ISPs

* Articles are numbered also using Japanese syllables (A,I,U,E,O,Ka,Ki,Ku,Ke,Ko,Sa,...). This figure lists information from the guidelines relating to each step in dealing with a DDoS attack. The text in each item summarizes that section, and may differ from the actual expressions used. The countermeasures detailed here are not approved unconditionally, and the decision of whether or not to employ them should be made on a case-by-case basis after comparing the situation that has occurred with the conditions and context in the guideline text, and referring to the examples given.

Figure 12: DDoS Attack Countermeasure Steps in the Guidelines

*[72] Self-defense (Penal Code Article 36), Averting Present Danger (Penal Code Article 37).

goes on to present an example of the former scenario where port 80 communications to a specific Web server IP address are blocked based on a user request, and an example of the latter scenario where IP packets with IP options that may adversely affect communications equipment are blocked. Furthermore, although Article 6 (2)-(Ki) "Blocking communications that spoof the sender" states that "using information relating to the sender's IP address to automatically block communications that spoof the sender constitutes the use of confidential communications without permission," it indicates that when the provider or user's equipment would be affected, such action would constitute legitimate self-defense or emergency measures. The example given explains actions corresponding to uRPF*[73] loose mode and strict mode.

When using these guidelines, it is sometimes necessary to combine multiple scenarios when evaluating criteria in addition to the individual questions presented here, such as when both the attacker and target are on a single ISP network.

■ Summary and Issues

These guidelines provide standards for determining what actions telecommunications carriers such as ISPs can take when an attack occurs, but providers are not meant to implement the measures detailed within in all cases. Providers must determine whether or not to implement countermeasures after taking into consideration the scale and nature of the attack as well as factors such as the cost of implementation. In order for the various countermeasures within to be implemented swiftly and without error, it will be necessary to continue evaluating implementation methods to cover more details, in particular with regard to requests from targeted parties*[74] and coordination between ISPs. We will continue to assess these issues through the activities of industry organizations such as Telecom-ISAC Japan.

1.5 Conclusion

This report has provided a summary of security incidents to which IIJ has responded. This time we discussed a series of attacks on companies and government organizations around the world that have taken place since the end of last year, and looked at guidelines for providers dealing with these kinds of attack. 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.

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

Hirohide Tsuchiya (1.2 Incident Summary)
Hirohide Tsuchiya, Hiroshi Suzuki, Tadaaki Nagao (1.3 Incident Survey)
Masafumi Negishi (1.4.1 Continuing Attacks on Companies and Government-Related Organizations)
Mamoru Saito (1.4.2 Guidelines for Dealing with High Volume Communications and Privacy at Telecommunications Carriers (Second Edition))
Office of Emergency Response and Clearinghouse for Security Information, IIJ Service Division

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

[73] Unicast Reverse Path Forwarding (uRPF). A technique defined in RFC3704 for suppressing communications from IP addresses that do not exist on routing information.

[74] Methods for coordinating with organizations such as ISPs when you are the target of a DDoS attack are examined in IIR Vol.9 (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol09.pdf) under "1.4.1 Preparing for DDoS Attacks on Small-Scale Systems".