

Large-Scale DDoS Attacks in the United States and South Korea

In this report, we will report on incidents to which IIJ responded between July and September 2009. At the same time, we will also cite the details behind large-scale DDoS attacks targeting Web servers in the United States and South Korea, TCP vulnerabilities announced by CERT-FI, and the mechanism behind silent phone calls caused by SIP packets.

1.1 Introduction

This whitepaper summarizes incidents to which IIJ responded, based on general information obtained by IIJ itself related to the stable operation of the Internet, information from observations of incidents, information acquired through our services, and information obtained from companies and organizations with which IIJ has cooperative relationships. This volume covers the period of time from July 1 through September 30, 2009. A multiple number of Web servers in the United States and South Korea were subject to large-scale DDoS attacks during this period. A series of vulnerabilities related to Web browsers were also discovered during this time, and reports cited a vulnerability in DNS servers and other servers used frequently for the Internet. Additionally, a TCP vulnerability that affects many implementations was announced. Besides these announcements and incidents, there were several incidents that resulted in direct financial damages, including cases of fake security software and extortion in connection with DDoS attacks. 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 July 1 and September 30, 2009. Figure 1 shows the distribution of incidents handled during this period.*1

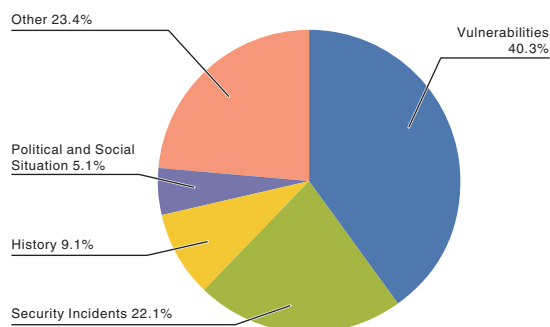


Figure 1: Incident Ratio by Category (July 1 to September 30, 2009)

*1 Incidents discussed in this whitepaper 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 an attack 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: Those incidents not directly associated with security problems, including highly concentrated traffic associated with a notable event.

■ Vulnerabilities

During this period, vulnerabilities were fixed in user applications such as Microsoft's Internet Explorer^{*2}, SMB2.0^{*3}, and Visual Studio Active Template Library^{*4}. Many vulnerabilities were also corrected related to Web browsers, including vulnerabilities in ActiveX killbit^{*5}, JScript^{*6}, Adobe Flash Player and Adobe Acrobat Reader^{*7}, and Apple QuickTime^{*8}.

In addition to the foregoing, vulnerabilities were discovered that affect the stability of BIND9^{*9}, Squid^{*10} and other software utilized frequently on servers. A Cisco router BGP vulnerability^{*11} was corrected, and a regular update for IOS was released to address several vulnerabilities during the period under study^{*12}. A vulnerability related to TCP was publicly announced, which affected a large number of implementations. See "1.4.2 TCP Vulnerability (Sockstress)" for more about this TCP vulnerability.

■ 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, Japan observed the 45th House of Representatives general election, the inauguration of the Consumer Affairs Agency, and other political events. However, IIJ noted no related Internet attacks.

■ History

The period in question included several historically significant days, including the observance of the end of World War II and the observance of the end of the Pacific War in Japan. In the past, historically motivated DDoS attacks and website alterations have occurred during this time of the year, and IIJ paid particular attention to political and social situations. However, no directly related attacks targeting IIJ facilities or customer networks were detected.

■ Security Incidents

Unanticipated security incidents not related to political or social situations occurred in the form of multiple large-scale DDoS attacks against web servers in the United States and Republic of Korea (South Korea) during the first part of July. See "1.4.1 DDoS Attacks in the United States and South Korea" for more related to these incidents. Additionally, attacks on P2P file sharing networks from a cloud environment^{*13} and a DDoS attack against Twitter^{*14} occurred. In August, a DDoS attack was accompanied by a demand for money, euphemistically called a cost of measures^{*15}.

-
- ^{*2} Microsoft Security Bulletin MS09-034 – Critical: Cumulative Security Update for Internet Explorer (972260) (<http://www.microsoft.com/technet/security/bulletin/ms09-034.mspx>).
- ^{*3} Microsoft Security Bulletin MS09-050 – Critical: Vulnerabilities in SMBv2 Could Allow Remote Code Execution (975517) (<http://www.microsoft.com/japan/security/Bulletin/MS09-050.mspx>).
- ^{*4} Microsoft Security Bulletin MS09-035 – Moderate: Vulnerabilities in Visual Studio Active Template Library Could Allow Remote Code Execution (969706) (<http://www.microsoft.com/technet/security/bulletin/ms09-035.mspx>) and Security Advisory for Adobe Flash Player APSA09-04 (<http://www.adobe.com/support/security/advisories/apsa09-04.html>).
- ^{*5} Microsoft Security Bulletin MS09-032 – Critical: Cumulative Security Update of ActiveX Kill Bits (973346) (<http://www.microsoft.com/technet/security/bulletin/MS09-032.mspx>).
- ^{*6} Microsoft Security Bulletin MS09-045 – Critical: Vulnerability in JScript Scripting Engine Could Allow Remote Code Execution (971961) (<http://www.microsoft.com/technet/security/bulletin/ms09-045.mspx>).
- ^{*7} Security advisory for Adobe Reader, Acrobat and Flash Player APSA09-03 (<http://www.adobe.com/support/security/advisories/apsa09-03.html>). Security updates available for Adobe Flash Player, Adobe Reader and Acrobat APSB09-10 (<http://www.adobe.com/support/security/bulletins/apsb09-10.html>).
- ^{*8} About the security content of QuickTime 7.6.4 (<http://support.apple.com/kb/HT3859>).
- ^{*9} BIND Dynamic Update DoS (<https://www.isc.org/node/474>). This vulnerability relates to a BIND server which holds zone information as a primary server. Even servers that provide only cache functions still frequently have zone information such as localhost, and need to be patched.
- ^{*10} Squid Proxy Cache Security Update Advisory SQUID-2009:2 (http://www.squid-cache.org/Advisories/SQUID-2009_2.txt).
- ^{*11} Cisco Security Advisory: Cisco IOS Software Border Gateway Protocol 4-Byte Autonomous System Number Vulnerabilities (<http://www.cisco.com/warp/public/707/cisco-sa-20090729-bgp.shtml>).
- ^{*12} Cisco Security Advisory: Summary of Cisco IOS Software Bundled Advisories, September 23, 2009 (<http://www.cisco.com/warp/public/707/cisco-sa-20090923-bundle.shtml>).
- ^{*13} A cNotes article reported this incident. Attacks on Share P2P networks utilizing Amazon Web Service (<http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=Amazon+Web+Service%A4%F2%CD%F8%CD%D1%A4%B7%A4%BFShare%A5%CD%A5%C3%A5%C8%A5%EF%A1%BC%A5%AF%A4%D8%A4%CE%B9%B6%B7%E2>)(in Japanese).
- ^{*14} Twitter's tweet discussing the status of ongoing denial-of-service attacks (<http://status.twitter.com/post/157191978/ongoing-denial-of-service-attack>). The Arbor Networks blog detailed the decrease in traffic volume "Where Did All the Tweets Go?" (<http://asert.arbornetworks.com/2009/08/where-did-all-the-tweets-go/>).
- ^{*15} See the following article from Trend Micro regarding similar incidents "Botnet Extortion Attempts Extend to Japan (DDoS Attacks)" (<http://blog.trendmicro.co.jp/archives/1385>)(in Japanese).

■ Other

As far as incidents not directly related to security, several international undersea cables were damaged by a typhoon in Taiwan, affecting communications in and out of the area^{*16}. A number of anti-virus software firms released 2010 updates, with concurrent releases of counterfeit software nearly indistinguishable from these programs^{*17}. Similarly, as Microsoft released its free Microsoft Security Essentials^{*18} anti-virus tool during the period under study, fake security software (scareware) began to appear in search engine results, inducing unsuspecting users to click through^{*19}.

1.3 Incident Survey

Of those 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 July 1 and September 30, 2009.

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.

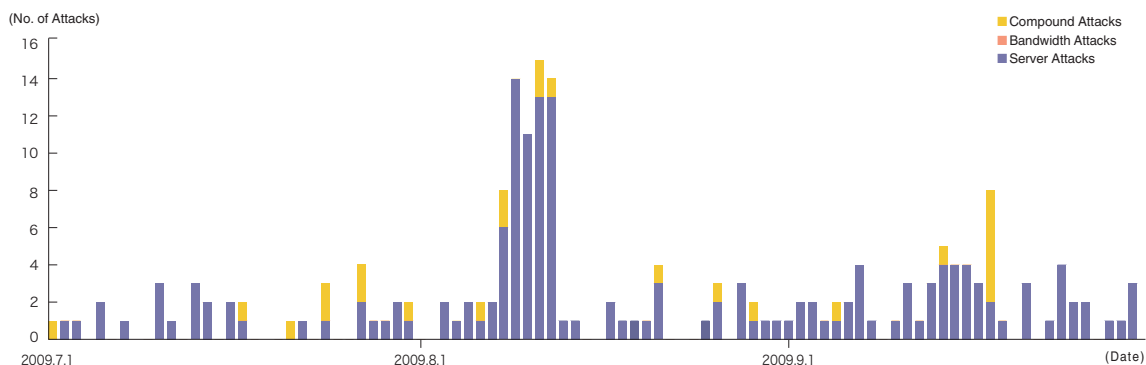


Figure 2: DDoS Attacks

*16 Reports about this incident include the following from NetworkWorld, "Asian undersea cable disruption slows Internet access" (<http://www.networkworld.com/news/2009/081209-asian-undersea-cable-disruption-slows.html>).

*17 Blog entry regarding counterfeit software accurately imitating Symantec products. Symantec Security Blogs: Nort "what" AV? (<http://www.symantec.com/connect/blogs/nort-what-av>).

*18 Microsoft Security Essentials (http://www.microsoft.com/security_essentials/).

*19 IIJ has confirmed that links leading to fake software have ranked high in English environment.

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^{*20}, attacks on servers^{*21}, 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 192 DDoS attacks. This averages to 2.08 attacks per day, representing an increase in the average daily number of attacks compared to our prior whitepaper. Considering the fact that a multiple number of attacks occurring between August 9 and August 12 targeted a certain website for a lengthy period, the overall trend did not otherwise vary significantly from that discussed in our prior whitepaper.

Bandwidth capacity attacks accounted for 0% of all incidents. Server attacks accounted for 87% of all incidents, and compound attacks accounted for the remaining 13%. The largest attack observed during the period under study was a compound attack that tied up 566Mbps of bandwidth using 140,000pps packets. Of all attacks, 80% ended within 30 minutes of commencement, while 19% lasted anywhere from 30 minutes to up to 24 hours. During the time period under study, IIJ noted one attack that lasted for 94 hours and 30 minutes (approximately four days).

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^{*22} and botnet^{*23} usage as the method for conducting DDoS attacks.

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the Malware Investigation Task Force (MITF)^{*24}, a malware activity observation project operated by IIJ. The MITF uses honeypots^{*25} 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.

^{*20} 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.

^{*21} 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.

^{*22} 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.

^{*23} 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."

^{*24} Malware Investigation Task Force (MITF). 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.

^{*25} 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 3 shows trends in the total volumes of communications coming into the honeypots (incoming packets) between July 1 and September 30, 2009. 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 client-targeted scanning behavior using TCP ports utilized by Microsoft operating systems. As with the prior study, we observed scanning behavior attempting to exploit 2967/TCP used by Symantec client software and 4899/TCP used by PC remote management tools. At the same time, communications for which the goal was not clearly identifiable, such as 53248/TCP and 20689/TCP (not used by general applications), were also observed. Attacks on 445/TCP, etc., targeting Microsoft vulnerabilities have continued since last October. Looking at the overall sender distribution by country, we see that attacks sourced to China and Japan, 26.6% and 24.4%, respectively, were comparatively higher than the rest.

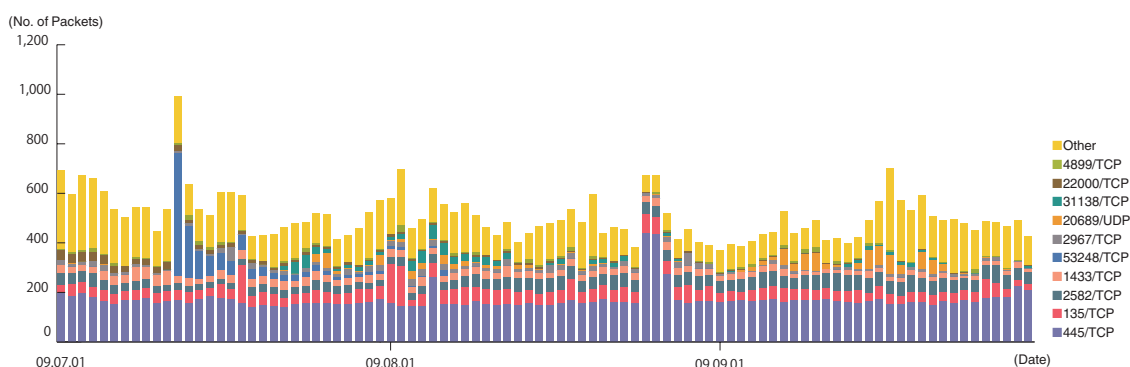


Figure 3: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

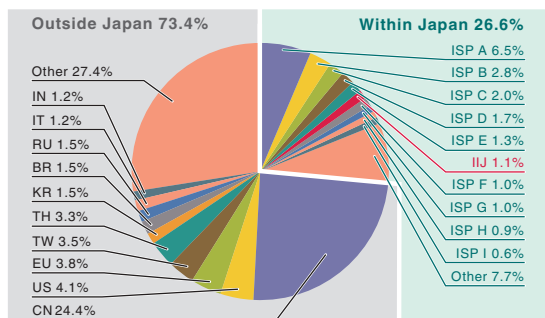


Figure 4: Sender Distribution (Entire Period under Study)

■ 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*²⁶, while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*²⁷.

On average, 592 specimens were acquired per day during the period under study, representing about 46 different malware variants. According to the statistics in our prior whitepaper, the average daily total for acquired specimens was 708, with 60 different variants, indicating a slight decline in average number of specimens and number of variants.

The distribution of specimens according to source country has Japan at 64.4%, with other countries accounting for the 35.6% balance. Of the total, malware infection activity among IJ users was 1.5%—a significant decrease compared to the 16.8% figure reported in our prior whitepaper. Looking more closely at the malware variants, after June of this year, we see that this trend has resulted from a dramatic decline in activities attempting to infect computers with Virut*²⁸ and its variants and activities related to Sdbot*²⁹ and its variants on the IJ network.

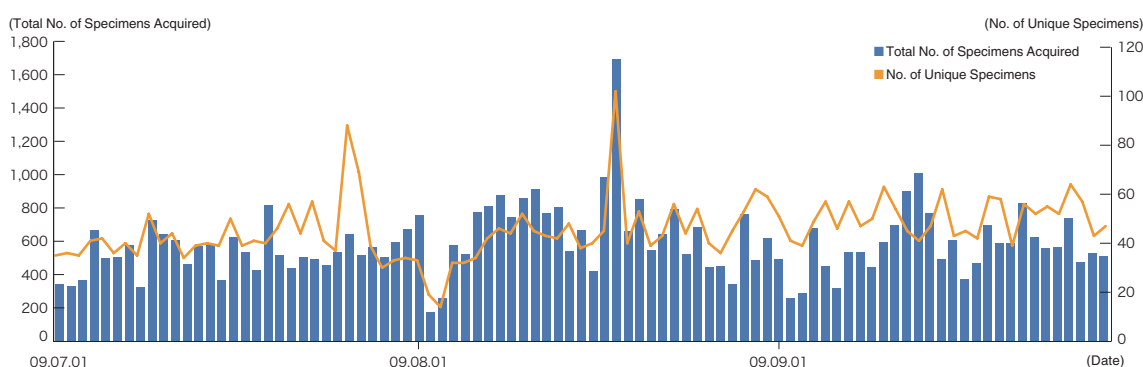


Figure 5: Trends in the Number of Malware Specimens Acquired (Total Number, Number of Unique Specimens)

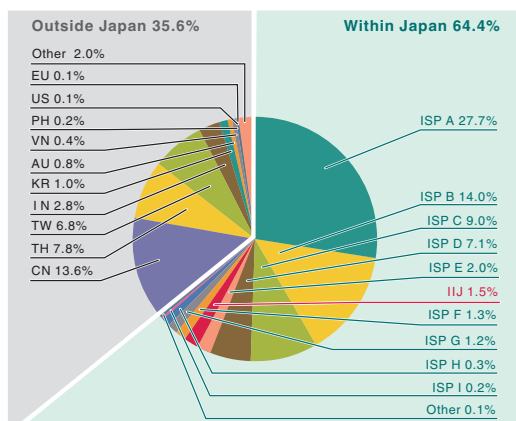


Figure 6: Distribution of Acquired Specimens by Source (Entire Period under Study)

*²⁶ This indicates the malware acquired by honeypots.

*²⁷ 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.

*²⁸ Virut is a virus spread through an infected file, and is not generally spread through networks. The propagation of this virus was attempted as the result of an attack exploiting a vulnerability. See Trend Micro's explanation of Virut (http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?vName=MAL_VIRUT). Also see an alert from the Information-Technology Promotion Agency, Japan (IPA) regarding Virut propagation via web content (<http://www.ipa.go.jp/security/txt/2009/03outline.html>) (in Japanese). A similar attempt to propagate malware was detected at the Cyber Clean Center, suspected to be related to other malware infection activities (<https://www.ccc.go.jp/report/200907/0907monthly.html>) (in Japanese).

*²⁹ An Sdbot is a type of bot conducting communications with the C&C server via IRC. See Trend Micro's explanation of the Sdbot (http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?vname=WORM_SDBOT.GEN).

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, 4.5% of the malware specimens were worms, 89.6% were bots, and 5.9% were downloaders. In addition, the MITF confirmed the presence of 44 botnet C&C servers^{*30} and 548 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^{*31}. 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 July 1 and September 30, 2009. Figure 8 shows the distribution of attacks according to source. These data are a summary of attacks detected by signatures on the IIJ Managed IPS Service. Japan was the source for 67.3% of attacks observed, while China and the United States accounted for 11.6% and 4.9%, respectively, with other countries following in order.

We noted a decrease in SQL injection attacks on web servers compared with our prior whitepaper. While the total number of SQL injection attacks declined, the decrease among source countries outside of Japan was particularly notable. Accordingly, the ratio of attacks sourced to Japan experienced a significant increase.

As previously shown, attacks of various types were properly detected and dealt with in the course of service. However, such attacks are constant and ongoing, calling for continued vigilance.

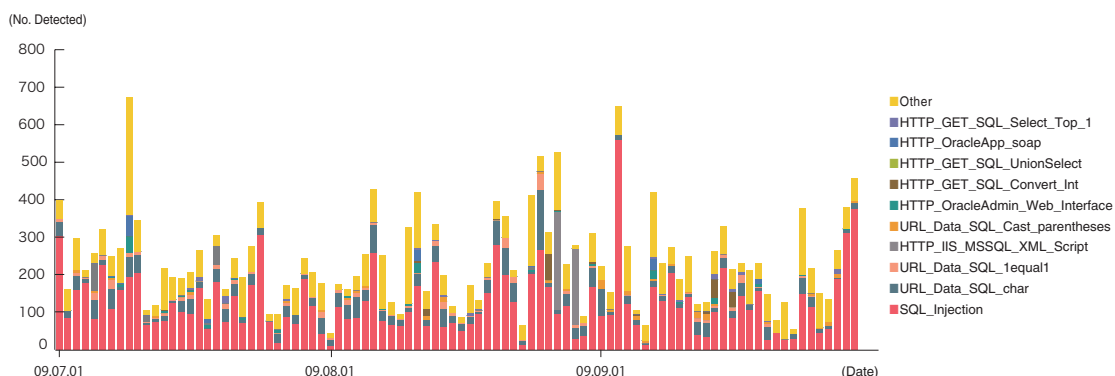


Figure 7: Trends in SQL Injection Attacks (by Day, by Attack Type)

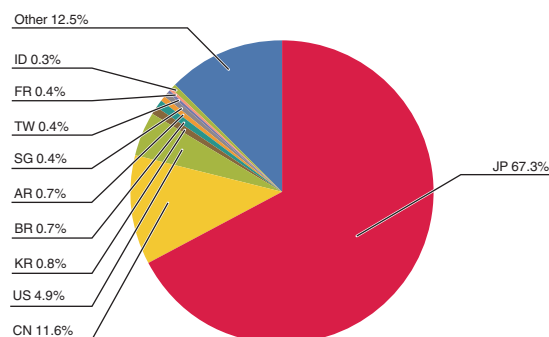


Figure 8: Distribution of SQL Injection Attacks by Source

^{*30} Abbreviation of "Command & Control." A server that provides commands to a botnet consisting of a large number of bots.

^{*31} 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 gathered from surveys performed during the period from July 1 and September 30, 2009 related to DDoS attacks in the United States and South Korea, TCP vulnerability (Sockstress), and randomly arriving SIP packets.

1.4.1 DDoS Attacks in the United States and South Korea

In early July 2009, websites in the United States and South Korea were victimized by a series of simultaneous DDoS attacks^{*32}. In this section, we will discuss the circumstances of these attacks, based on information obtained by IIJ.

■ DDoS Attack Background

This particular series of DDoS attacks did not use botnets so widely encountered today, but rather malware designed specifically for these attacks. It is reported that this specially designed malware propagated through websites inside South Korea used for file sharing^{*33}. Because of this, many of the IP addresses traced as the source of the attack reportedly have been identified as South Korean IP addresses^{*34}. Malware files of a similar type were placed on similar web services outside South Korea, infecting PCs in other countries^{*35}. While it is unclear as to what timeframe these infection activities took place, it is believed that the propagation activities took place in a concentrated period immediately before the DDoS attacks in order to evade detection and countermeasures by anti-virus software vendors^{*36}. The total number of PCs infected by the malware is undetermined, but a subsequent announcement out of South Korea indicated that the infection affected approximately 78,000 machines within the country^{*37}.

The DDoS attacks first occurred on July 5^{*38} and July 6 (Korean time), mainly targeting multiple government agencies' web servers in the United States. After July 7, the attacks moved to multiple websites in South Korea. The attacks in South Korea affected not only government agencies, but also online banking sites, webmail services, and other popular online consumer services. It has been reported that the infected PCs used for the DDoS attacks did not generate significant amounts of traffic singly. Rather than occupying communication lines using massive volumes of traffic, the attacks mainly put a direct load on the target servers^{*39}.

This particular DDoS attack died down on July 10, eventually running its course^{*40}. That the malware was cleaned from 95% of the approximately 78,000 machines infected within four days was mostly due to the efforts of South Korean ISPs, security organizations, and media^{*41}. As a result of these efforts, the DDoS attack converged as of July 10. There was a report that only several hundred hard drives were destroyed as a side effect of infection with the malware.

^{*32} F-Secure reported on its blog that several websites in the United States became inaccessible because of this DDoS attack (<http://www.f-secure.com/weblog/archives/00001720.html>). South Korean news organizations also reported that several websites in that country became inaccessible due to the attack.

^{*33} Web-based file-sharing services (so-called "uploaders" in Japan) are used frequently in South Korea by corporations and educational institutions. It is believed that many users became infected when files containing the malware infection package were uploaded to several of these services.

^{*34} The following report states that more than 100,000 PCs were conscripted in this attack, between 90% and 95% of which were located in South Korea (<http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20090710>).

^{*35} The following is an alert from JPCERT/CC discussing the attack from Japan, "DDoS attack against Web sites in South Korea and US" (<http://www.jpcert.or.jp/at/2009/at090012.txt>) (in Japanese).

^{*36} As one circumstantial evidence, a specimen obtained and studied by IIJ forged a file creation date of 2004, while the time stamp in the PE header of each file showed a date immediately prior to the launch of the attack, "July 4, 2009 0:38" for `perfvwr.dll` as an example.

^{*37} Information related to the number of affected machines inside South Korea is detailed in a presentation at APNIC28 by KRNIC of KISA (Korean Internet & Security Agency) (http://meetings.apnic.net/_data/assets/pdf_file/0019/14077/lee-ddos-attack.pdf).

^{*38} The first attack began at 2am, July 5 Korean local time. The time was 13:00 EDT July 4 (Independence Day) in the United States. There is no time zone difference between Korea and Japan.

^{*39} For example, the following alert from KrCERT indicates the circumstances of the DDoS attack traffic from this malware (<http://www.krcert.or.kr/noticeView.do?num=340>). (in Korean)

^{*40} With traffic returning to normal levels, the Korean NCSC (National Cyber Security Center) lowered its warning level from an "alert" to a "notice" on July 12.

^{*41} According to the details published by KrNIC in APNIC28 (<http://meetings.apnic.net/28/program/apops/transcript#ji-young-lee>). Subsequent to the DDoS attack in South Korea, information about the malware used in the attack and tools dedicated to eliminate the malware were promptly provided by several anti-virus vendors. Television news programs and popular web services issued notifications regarding the attack in conspicuous ways in efforts to alert the public and publicize information regarding corrective action. Information was also released notifying users that backing up their system clocks to an earlier time was an effective temporary measure against one of the malware variants that would destroy hard drives on a specific date (July 10).

■ Malware used in the DDoS Attacks

Once this attack occurred, IIJ first obtained several malware specimens from general malware-related information sources and organizations. These specimens included malware that first induces malware infections for DDoS attacks, malware containing functions for actual DDoS attacks and malware that continues to update attack targets.

Having analyzed and conducted demonstration tests on these specimens, we learned that the malware utilized in these attacks behaved as shown in Figure 9^{*42}.

First, the initial malware package (msiexec*.exe, etc.) drops (creates) two types of malware (perfvwr.dll (or wmiconf.dll) and wmcfg.exe) (1). The malware perfvwr.dll (or wmiconf.dll) first turns off the personal firewall of the infected PC prior to commencing the attack. Next, the infected PC connects to three separate servers, creating a configuration file (uregvs.nls) for the attack (2). The perfvwr.dll and wmiconf.dll malware files start a DDoS attack according to the configuration file (3). The configuration file contains the length of time, target server, attack type and number of attacks for the DDoS attack. This malware-based attack is performed as shown in Figure 9 (4), in accordance with the configuration file. The results of the IIJ demonstration tests showed that the attack traffic generated per machine was 110pps for TCP SYN flood, 110pps for TCP ACK flood, and around 216pps for UDP and ICMP floods, with 107cps (commands per second) for HTTP GET flood and HTTP POST flood. We also observed behavior of intermittent increases and decreases in communications via program-embedded temporary suspension command.

Meanwhile, wmcfg.exe drops two more files—mstimer.dll and wversion.exe (5). The mstimer.dll file downloads a file called flash.gif from multiple web servers (6), extracting and updating a file called wversion.exe from flash.gif (7), while at the same time sending spam to multiple addresses (8). The wversion.exe file deletes the mstimer.dll file and itself, removing evidence (9). However, a function is inserted after the update to search and destroy files on the hard drive having certain extensions (10), writing certain character strings to the hard drive MBR^{*44}, and preventing the PC from being turned on (11).

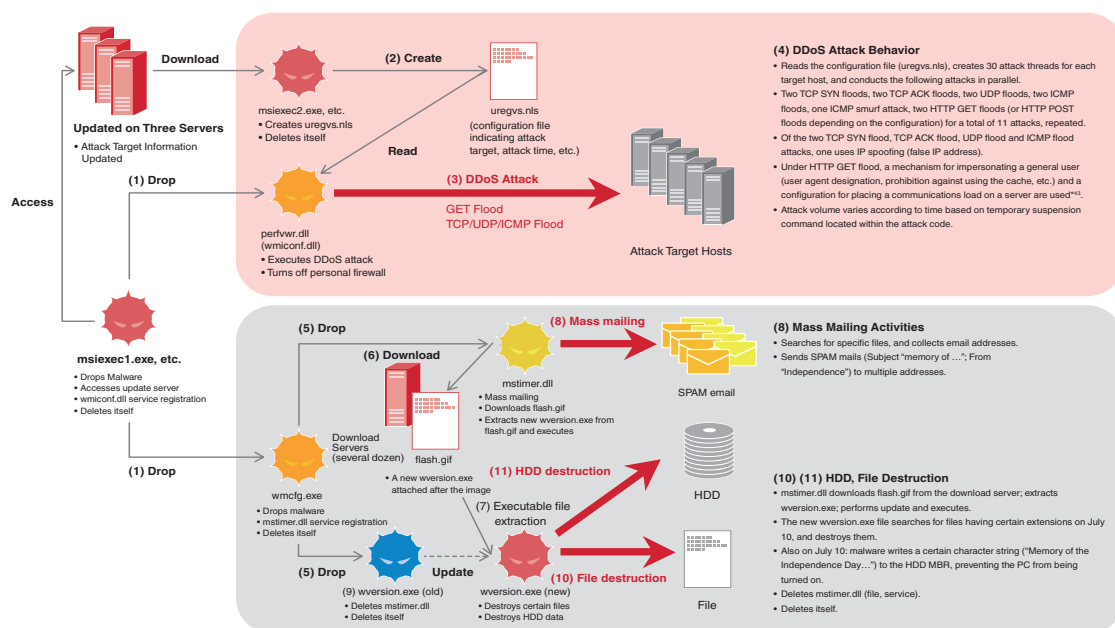


Figure 9: Behavior of Malware used in DDoS Attacks

^{*42} Our descriptions of this behavior is based on our best efforts at directly gathering information; however, the description includes some information that IIJ was not able to directly confirm about the roles and status of various Internet servers at the time of the DDoS attack.

^{*43} Various patterns were noted; character strings forged Firefox, IE7.0, or IE8.0 in the User-Agent header. "ko" (Korean language) was designated in the Accept-Language header. The Cache-Control header of some requests showed no-store, must-revalidate.

^{*44} MBR: Acronym for Master Boot Record. The MBR is a region at the front of the hard drive; normally programs used for launching the computer's operating system are stored in this region.

■ Summary of the Attack

Figure 10 shows the chronological order of the progression and related events for the attack described in this section.

Normally, DDoS attacks are designed for harassment or other clear intent targeting a certain website, and are generally one type of security incident for which the purpose is comparatively easy to identify. The DDoS attack described here, however, was highly complex (malware propagates within South Korea first, attacks targets in the U.S. and then South Korea^{*45} and intervening malware divides into two independent malware packages, etc.) and the purpose was difficult to identify.

■ Measures against This Particular Type of DDoS Attacks

Here, we will consider the difference between the measures against the damages incurred due to this particular DDoS attack and those that would normally be taken against a DDoS attack. This attack consisted of the mass operations of numerous PCs infected with the malware, making it difficult to institute access or bandwidth controls for the individual PC IP addresses from which the attack traffic was generated. However, much of the attack traffic originated from within one country, and performing access and bandwidth controls on a network basis appeared to be an effective temporary countermeasure. A characteristic of this incident was the low volume of attack traffic from individual PCs infected with the malware. In particular, the web requests involved in the attack were disguised to imitate user behavior, making the determination between normal and attack traffic comparatively difficult. Even if anti-DDoS equipment were available, some adjustments would have been required to establish the abnormal behavior detection threshold and operating mode configurations.

At IIJ, we believe it is necessary to research measures that would deal with this type of DDoS mechanism if such an attack were to take place within Japan. Where the malware executed an attack based on a configuration file distributed beforehand, rather than dealing with the attack by taking action against a centrally controlled botnet, the only solution for stopping such an attack is to eliminate the malware on each individually infected PC. As we saw take place in South Korea, to promptly delete the malware from so many individual PCs requires the cooperation and coordination of many different organizations. To be able to accomplish something on this scale, organizations must be vigilant and ready to engage in synergistic action when called for^{*46}.

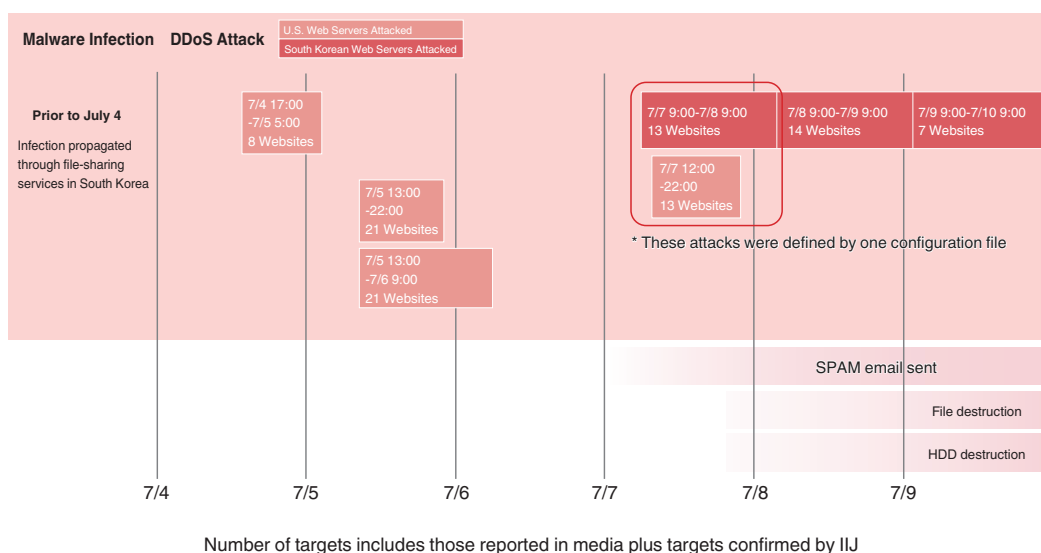


Figure 10: DDoS Attacks against the United States and South Korea: Chronological Order (UTC)

^{*45} According to the specimen acquired, 13 U.S. websites (from July 7, 2009 18:00 to July 8 18:00) and 13 South Korean websites (from July 7, 2009 21:00 to July 8 7:00) were attacked under the configuration in the same file. We see that this is the dividing line between where the attacks transitioned to domestic South Korean servers.

^{*46} In Japan, cyber security exercises have been conducted such as those sponsored by "Anti-Cyber Attack Exercises in the Telecommunications Business Sector" (http://www.soumu.go.jp/menu_news/s-news/2006/061201_4.html) (in Japanese) of the Ministry of Internal Affairs and Communications, and those by Telecom-ISAC Japan (<https://www.telecom-isac.jp/english/index.html>). There also have been international exercises including APCERT drills (<http://www.apcert.org/documents/pdf/APCERT-drill-2008.pdf>). IIJ actively participates in these exercises.

1.4.2 TCP Vulnerability (Sockstress)

In September 2009, Finnish CSIRT organization CERT-FI published the state of the response to vulnerabilities related to TCP.

^{*47} This announcement was picked up widely in the press. In this section, we will explain these TCP vulnerabilities and responses.

■ Background

The vulnerabilities themselves were first identified one year prior to the Finnish announcement. Two researchers from a security vendor Outpost24 first identified the issue. These researchers developed a tool to speed up network scanning called Unicornscan^{*48}. During their use of this new tool, they happened to notice unexpected behavior in TCP, and created a tool called Sockstress^{*49} to generate traffic that exploited this behavior (this tool has not been publicly released).

Based on the information demonstrating the existence of these vulnerabilities, CERT-FI took the lead in organizing a community that encouraged product developers to take appropriate measures. In Japan, this issue is being handled by the Information Security Early Warning Partnership^{*50}.

■ Details of the Vulnerabilities

The tool for exploiting these vulnerabilities (Sockstress) has not been released to the public, nor have the complete details about these vulnerabilities been disclosed. Here, we offer a commentary regarding “zero window size,” which has been most widely discussed in the public.

An attack using zero window size occurs as follows:

1. Establish a TCP connection from a client to a server.
2. During communications, the client specifies zero as its receive window size to declare “buffer full, cannot receive any more data.” In this state, the server will temporarily suspend data transmission via this TCP connection. The server will continue to query the current client-side receive window size in certain intervals, maintaining the connection as long as a response is received.
3. Steps 1 and 2 above from client to server are repeated over and over again.
4. Server resources are exhausted, and new TCP connections cannot be accepted.

In fact, the time for an attack to become effective depends on the server implementation, resources and capacity. It is also possible that while the load climbs high, an attack doesn't become successful.

Maintaining a connection under a zero window size state is actually a normal operation under TCP standards RFC793^{*51} and RFC1122^{*52}. Even regular clients using TCP for

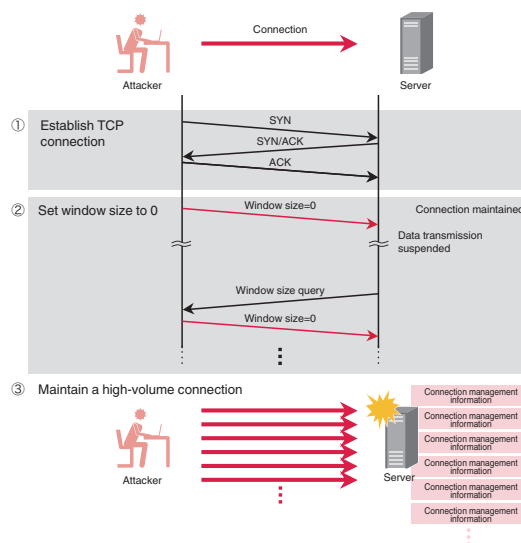


Figure 11: Server-side stack through zero window size designations

^{*47} Response to TCP vulnerabilities (<https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html>) (<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4609>) (<http://www.microsoft.com/technet/security/bulletin/ms09-048.mspx>), etc.

^{*48} Unicornscan (<http://www.unicornscan.org/>).

^{*49} While Sockstress itself has not been released publicly, related information has been summarized (<http://sockstress.com/>).

^{*50} The Information Security Early Warning Partnership is a framework for vulnerability information dissemination to product developers based on the Ministry of Economy, Trade and Industry directive #235. Under this partnership, the IPA (http://www.ipa.go.jp/security/english/quarterlyrep_vuln.html#Partnership) acts as the vulnerability information reception agent, while the JPCERT Coordination Center (<http://www.jpcert.or.jp/english/vh/project.html>) serves as the coordinating agent to product developers. Information about vulnerabilities is published through JVN (<http://jvn.jp/en/>). IIJ participates in this partnership as a developer of proprietary router and other products.

^{*51} RFC793 Transmission Control Protocol (<http://www.ietf.org/rfc/rfc793.txt>).

^{*52} RFC1122 Requirements for Internet Hosts - Communication Layers (<http://www.ietf.org/rfc/rfc1122.txt>).

communications can designate zero window size as normal communications control. The issue pointed out here is that the designation of zero window size can be used to mount an attack, presenting a method that forces the server to maintain TCP connections at volumes exceeding system resources. However, this zero window size attack is not a new method. For example, the IETF^{*53} TCPM Working Group^{*54} broached this subject in July 2006^{*55}, well before the advent of Sockstress.

■ A Protocol Issue or an Implementation Issue?

As shown above, the zero window size designation is a normal state according to protocol specifications. However, a large volume of TCP connections in this state is seen as an issue. To resolve this issue, arguments call for either making changes to the TCP protocol itself, or establishing a timeout value or other adjustment in the implementation as a workaround.

Arguments in the earlier-mentioned IETF TCPM Working Group state that this type of attack is an issue of the OS or server implementation resource management. The consensus is that the solution should be made within implementation in consideration of individual circumstances, rather than treating this as a protocol issue.

■ Effectiveness of Countermeasures

IIJ picked up the Microsoft patch as one means of dealing with this zero window size issue and performed demonstration tests of an implementation before and after applying the patch. Figure 12 shows the results of this test^{*56}.

As shown in the results of this test, the patched implementation demonstrates a stronger resistance to this type of attack. However, this countermeasure forces the termination of existing TCP connections to make room in resources to accept new connections. We have to admit that important connections may also be unavoidably terminated. This countermeasure does not completely prevent this type of attack. Not only Microsoft, but many of the other entities publishing a patch dealing with this issue have adopted measures that similarly control the usage of limited resources.

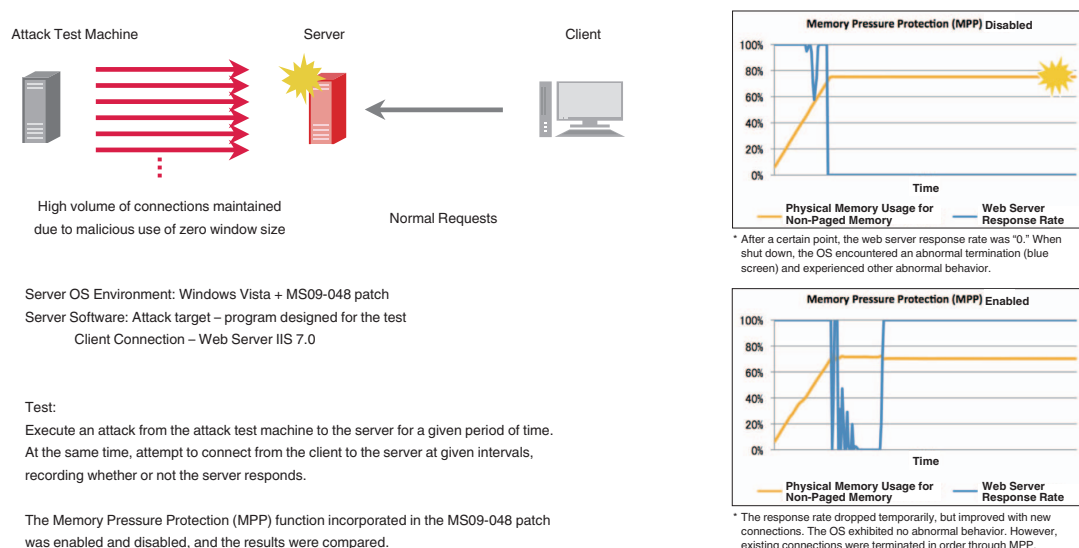


Figure 12: Demonstration Test and Results

*53 IETF is the acronym for the Internet Engineering Task Force. An organization that develops the standardization of Internet technologies. (<http://www.ietf.org/>)

*54 TCPM is a short name for TCP Maintenance and Minor Extensions Working Group (<http://www.ietf.org/dyn/wg/chapter/tcpm-charter.html>).

*55 Discussion launched on the TCPM WG mailing list (<http://www.ietf.org/mail-archive/web/tcpm/current/msg02189.html>) and subsequently submitted Internet Draft "Clarification of sender behavior in persist condition" (<https://datatracker.ietf.org/drafts/draft-ananth-tcpm-persist/>), etc.

*56 In fact the Microsoft Web Server, Internet Information Service (IIS) includes functions to adjust web response according to OS load status. Simply performing the attack in question on the Web Service did not result in abnormal OS behavior. Accordingly, this experiment used this attack to place loads on other services.

As we have shown, this issue has been treated as an implementation vulnerability. However, because one cannot tell an attack connection from a normal connection from TCP standards, one has to conclude that this is an issue of system resource management for systems that receive a large volume of connections. There might be other similar issues that cannot be fundamentally resolved through implementation modifications^{*57}, and it is likely that more will be uncovered in the future. Accordingly, servers open to the Internet must be carefully operated continuously.

1.4.3 Randomly Arriving SIP Packets

■ Fraudulent SIP Communications

From last year, IIJ has continued to observe SIP (Session Initiation Protocol)*⁵⁸ packets intermittently arriving at honeypots. These SIP packets were sent to large numbers of IP addresses across the Internet, attempting to connect to terminals that could interpret SIP. Depending on the configuration, certain VoIP routers and IP telephones play a ring alert merely at the arrival of these SIP packets. This was the underlying cause behind the large number silent call reports*⁵⁹.

■ SIP-Based VoIP Communication Mechanism

As indicated by the name, SIP is one protocol used to control a session, based on a request-and-response model similar to HTTP. SIP is used in IP phone services and other VoIP communications. However, while the HTTP specification defines data transmission as well, SIP only controls the initiation, modification, and termination of a session between VoIP terminals, leaving data transmission to other protocols such as Real-time Transport Protocol (RTP)^{*60} for audio, etc. Figure 13 shows an example of SIP communications via IP telephone.

- (1) When a call is initiated via IP telephone, the origin of the call (User Agent:UA) first sends an INVITE message to the call receiver.
- (2) When the call receiver gets the INVITE message, a ring tone is sounded to notify the called user. At the same time, “180Ringing” (meaning that a call is in progress) is returned to the originator of the INVITE message.
- (3) When the call target picks up the receiver, the receiving terminal sends a 200 OK message to the originator of the call.
- (4) Having received this message, the originator of the call sends an ACK response to the call receiver, and the session is established.

This is the basic operation. In general, SIP servers are used when connecting, rather than directly connecting the two terminals^{*61}.

■ Attacks Targeting IP-PBX

To control adoption and maintenance costs, more corporations today are replacing existing PBX*⁶² systems with IP phone systems using IP-PBX*⁶³. With the availability of low-cost IP-PBX appliances, it is likely that this trend will continue to gather momentum.

While IP-PBX does present significant adoption benefits in terms of cost savings, different than existing telephone networks, IP-PBX is connected to a network that features other connections with non-VoIP equipment, including the

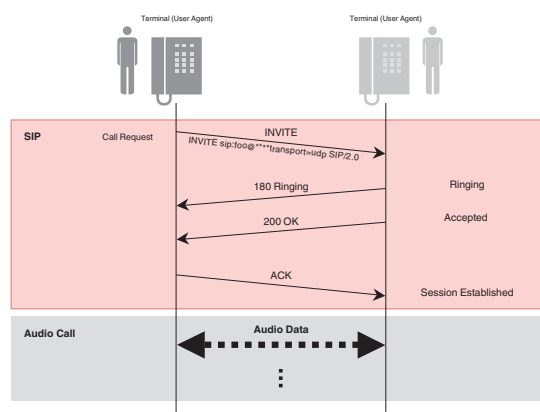


Figure 13: Initiating SIP-Based Audio Communications

*57 For example, a survey report on TCP robustness by CPNI of United Kingdom (<https://www.cpni.gov.uk/Docs/tn-03-09-security-assessment-TCP.pdf>) and a summary survey report of existing TCP/IP vulnerabilities by the IPA (http://www.ipa.go.jp/security/vuln/vuln_TCP/IP.html) (in Japanese). These reports publicized several of these issues, providing developers with commentary on important points related to TCP/IP protocol stack implementations. The latter report also includes a guide for system operators.

*58 We also addressed random SIP packets in Vol.4 of this report (http://www.ijl.ad.jp/en/development/iir/pdf/iir_vol04_EN.pdf).

*59 For example, a cNotes article reported this incident: "INVITE Flood? Fraudulent SIP Calls" (<http://jvnrrs.ise.chuo-u.ac.jp/csn/index.cgi?p=INVITE+Flood%3F+%C9%D4%C0%B5%A4%CASIP%C3%E5%BF%AE>) (in Japanese).

*60 Real-time Transport Protocol is a data transfer protocol for transmitting a data stream in real time. Used for audio and video transmission, most VoIP equipment supports RTP.

*61 An SIP server includes proxy, redirect, and register functions; normally, communications with another party are handled via SIP servers.

*62 A PBX (Private Branch eXchange) is a telephone exchange local to a particular office. It connects internal and external (public switched telephone network) lines and controls incoming and outgoing calls.

*63 A PBX that includes VoIP functions. Asterisk (<http://www.asterisk.org/>) is one example.

Internet, and closed IP networks. Because of this, one must consider the fact that the IP-PBX is more susceptible to external and internal attacks than a traditional PBX. Most of today's VoIP products utilize SIP on UDP; accordingly, SIP packets with false IP addresses and caller phone numbers can be easily created. In fact, there have been cases overseas of hackers exploiting vulnerabilities to fraudulently operate an IP-PBX, capturing IP telephone service contract information in an attempt at fraudulent use^{*64}. Other cases have involved numerous phone calls with false caller numbers, attempting to have the callees call back to premium toll numbers, thus fraudulently building up charges and stealing money^{*65}. The random SIP packets observed by IIJ were not for the purpose of causing silent calls, but more likely attempts to find IP-PBXs having an exploitable vulnerability.

■ VoIP Security Countermeasures

It is vital to always operate equipment correctly and securely. For example, gain a correct understanding of the types of threats involved^{*66}, receive periodic updates regarding recommended settings and product information from your VoIP equipment vendor, confirm important issues related to service usage with your ISP, etc. If possible, configure VoIP equipment with encryption functions, enable settings to only accept SIP packets from certain SIP servers, and incorporate other appropriate access controls via functions and settings to prevent SIP messages from unknown sources. Adopting VoIP-compatible firewalls, IDS and IPS, as well as a session border controller^{*67} is also an effective preventive measure.

We believe that the growth of VoIP will continue, along with increasingly widespread adoption of personal-use IP phones and corporate IP-PBXs. On a traditional phone, users would hesitate to answer a call coming in from a complete stranger. This same caution should apply to both traditional and newly emerging threats involved in VoIP communications.

1.5 Conclusion

This whitepaper has provided a summary of security incidents to which IIJ has responded. In this volume, we have included security incidents in which IIJ was not directly involved, mainly addressing the DDoS attacks in the United States and South Korea. We believe that our mission encompasses the collection and analysis of information stemming from incidents that occur in other countries to be better able to rapidly respond should a similar incident occur in Japan in the future.

By identifying and publicizing incidents and associated responses in whitepapers 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.

Authors:

Mamoru Saito

General Manager of the Division of Emergency Response and Clearinghouse for Security Information, IIJ Service Business Department- 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, 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 DDoS Attacks in the United States and South Korea)

Tadaaki Nagao, Yuji Suga (1.4.2 TCP Vulnerability (Sockstress))

Hirohide Tsuchiya (1.4.3 Randomly Arriving SIP Packets)

Division of Emergency Response and Clearinghouse for Security Information, IIJ Service Business Department

Contributors:

Shigeki Ohara System Development Section, System Infrastructure Division, IIJ Service Business Department

Masahiko Kato, Masafumi Negishi Division of Emergency Response and Clearinghouse for Security Information, IIJ Service Business Department

^{*64} For example, an alert issued by the Internet Crime Complaint Center (IC3: an organization involved in combating cyber crime) in cooperation with U.S. law-enforcement agencies (FBI, etc.) (<http://www.ic3.gov/media/2008/081205-2.aspx>).

^{*65} The F-Secure blog post "Beware of One-Ring Fraud," (<http://www.f-secure.com/weblog/archives/00001744.html>) for example.

^{*66} See the following report as one source of information regarding known vulnerabilities and threats. "Survey Report regarding Known SIP Vulnerabilities Version 2.0" by the IPA. (http://www.ipa.go.jp/security/vuln/vuln_SIP.html) (in Japanese).

^{*67} A device installed at the boundary of the VoIP network. Responsible for controlling necessary ports according to SIP packet content, and for controlling functions allowing for normal VoIP communications, even in a NAT environment.