Renewed Gumblar Activity

In this whitepaper, we will report incidents that occurred between October and December 2009, in addition to commenting on Gumblar-related incidents that have been re-occurring since October, vulnerabilities in the SSL and TLS protocols that are widely used for encrypted communications, and techniques for surveying P2P file sharing networks.

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 October 1 through December 31, 2009. In this period the Gumblar malware that steals IDs and passwords re-emerged, and many website alterations related to this have been reported. A series of vulnerabilities related to Web browsers were also discovered, in addition to an issue with the SSL and TLS protocols that are widely used for encrypted communications. Besides these there was also a hijacking incident in which DNS information was manipulated without authorization, and SEO poisoning incidents that took advantage of a natural disaster. 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 October 1 and December 31, 2009. Figure 1 shows the distribution of incidents handled during this period[1].

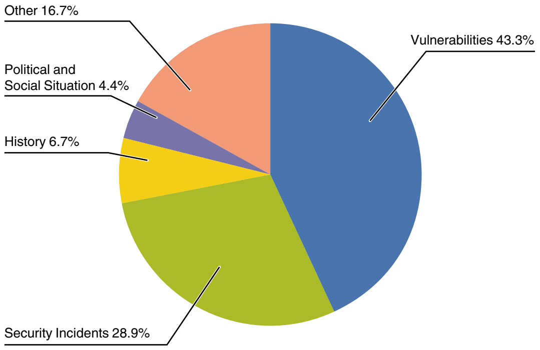


Figure 1: Incident Ratio by Category (October 1 to December 31, 2009)

[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 attacks in connection with a past historical fact.
Security Incidents: Wide propagation of network worms and other malware; DDoS attacks against certain websites. Unexpected incidents and related response.
Other: Those incidents not directly associated with security problems, including highly concentrated traffic associated with a notable event.

■ Vulnerabilities

During this period a large number of Web browser-related vulnerabilities were discovered and fixed, including Microsoft's Internet Explorer*[2], Adobe Systems' Adobe Acrobat, Adobe Reader*[3], Adobe Flash Player, Adobe AIR*[4], and Adobe Shockwave Player*[5], and Oracle's Java Runtime Environment (JRE)*[6]. Several of these vulnerabilities were exploited before patches were released*[7].

Vulnerabilities were also discovered and fixed in widely used servers such as NTP*[8] used for time synchronization, and BIND9*[9] DNS servers. Additionally, a vulnerability was discovered in the SSL and TLS protocols*[10] that are utilized for encrypted communication by many services. See "1.4.2 MITM Attacks Using a Vulnerability in the SSL and TLS Renegotiation" for more information about this 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 IIJ observed visits to Japan by foreign VIPs, such as US President Obama in November and Chinese Vice-President Xi Jinping in December, but no related attacks were noted.

■ 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 the discovery of malware that infects the Apple iPhone*[11]. There was also an incident where DNS information for the popular Twitter SNS was manipulated without authorization, causing traffic to be redirected to another website*[12]. Incidents of users being induced to download fake security software (scareware) through search engine results continued to occur*[13].

Additionally, the Gumblar*[14] malware that was active on a large scale in April resurfaced at the beginning of October. See "1.4.1 Renewed Gumblar Activity" for more information about this.

*2 Microsoft Security Bulletin MS09-072 – Critical: Cumulative Security Update for Internet Explorer (976325) (http://www.microsoft.com/technet/security/bulletin/ms09-072.mspx).

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

*4 Security updates available for Adobe Flash Player APSB09-19 (http://www.adobe.com/support/security/bulletins/apsb09-19.html).

*5 Security updates available for Shockwave Player APSB09-16 (http://www.adobe.com/support/security/bulletins/apsb09-16.html).

*6 Oracle Corporation, "JavaTM SE 6 Update Release Notes" (http://java.sun.com/javase/6/webnotes/6u17.html).

*7 A zero-day attack is the exploitation of software vulnerabilities for which no fix is available yet. For example, during this period IIJ confirmed incidents of Gumblar and other malware exploiting vulnerabilities in Adobe Reader and Acrobat before a patch was released. These vulnerabilities could be worked around even before a patch was released by prohibiting the use of JavaScript in the settings for Adobe Reader and Acrobat.

*8 Vulnerability Note VU#568372, "NTP mode 7 denial-of-service vulnerability" (http://www.kb.cert.org/vuls/id/568372). By sending specially crafted request packets to an NTP server, it is possible to create an infinite loop repeating responses and requests.

*9 Vulnerability Note VU#418861, "BIND DNS Nameserver, DNSSEC validation Vulnerability" (http://www.kb.cert.org/vuls/id/418861). There is a risk of cache poisoning when using DNSSEC.

*10 Vulnerability Note VU#120541, "SSL and TLS protocols renegotiation vulnerability" (http://www.kb.cert.org/vuls/id/120541).

*11 Details regarding this worm can be found on the F-Secure Corporation blog. "First iPhone Worm Found" (http://www.f-secure.com/weblog/archives/00001814.html).

*12 See the following official blog for details regarding the effects of this attack. Twitter blog, "Update on Last Night's DNS Disruption" (http://blog.twitter.com/2009/12/update-on-last-nights-dns-disruption.html).

*13 SEO poisoning is the act of using a search engine ranking algorithm to display links to malicious sites at the top of search results for certain phrases. For example, the Trend Micro blog below carried out a survey and analysis of words often used in searches during the Christmas season. Trend Micro Incorporated, "SEO poisoning: malicious sites also using SEO marketing?" (http://blog.trendmicro.co.jp/archives/1255) (in Japanese). For the current incidents phrases related to the earthquake that occurred near the Samoan Islands on September 30, 2009 were the target of SEO poisoning.

*14 Gumblar is also explained in Vol.4 of this whitepaper: "1.4.2 ID/Password Stealing Gumblar Malware" (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol04_EN.pdf).

■ **Other**

As far as incidents not directly related to security, a popular Internet message board restricted access from multiple ISPs on a large scale, hindering consumer usage.

Additionally, because many attacks exploiting vulnerabilities in user applications such as Web browser plug-ins occurred during this period, tools for confirming the version of applications and plug-ins have been released (IPA MyJVN Version Checker*[15] and Firefox PluginChecker*[16], etc.). Microsoft's new Windows 7 operating system was also released, and was hailed for its improved security features.

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 October 1 and December 31, 2009.

*15 MyJVN Version Checker enables users to confirm the version of certain software applications installed on the PC they are using (http://jvndb.jvn.jp/apis/myjvn/) (in Japanese).

*16 Visit the following URL using Mozilla Firefox (https://www-trunk.stage.mozilla.com/en-US/plugincheck/). It is also possible to confirm whether or not updates are available by clicking the "Tools (T)" menu, and then selecting "Add-ons (A)." This is a Firefox function, so different methods will be required to confirm plug-ins for other browsers, such as Microsoft Internet Explorer.

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

There are many methods that can be used to carry out a DDoS attack. In addition, the capacity of the environment attacked (bandwidth and server performance) will largely determine the degree of impact. Figure 2 categorizes DDoS attacks into three types: attacks on bandwidth capacity*[17], attacks on servers*[18], 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 185 DDoS attacks. This averages to 2.01 attacks per day, indicating that there was no significant change in the average daily number of attacks compared to our prior whitepaper.

Bandwidth capacity attacks accounted for 0.5% of all incidents. Server attacks accounted for 87.6% of all incidents, and compound attacks accounted for the remaining 11.9%. The largest attack observed during the period under study was a server attack that resulted in 245Mbps of bandwidth using 650,000pps packets. Of all attacks, 77% ended within 30 minutes of commencement, while 23% lasted between 30 minutes and 24 hours. The longest sustained attack lasted for approximately 12 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*[19] and botnet*[20] usage as the method for conducting DDoS attacks.

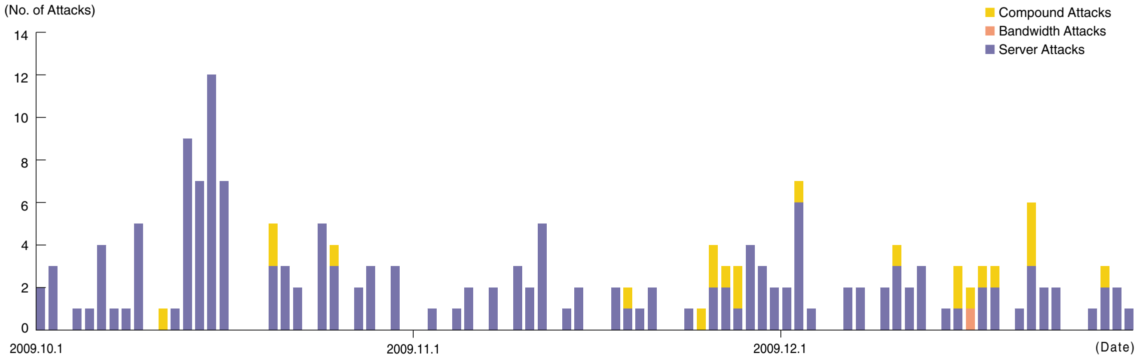


Figure 2: Trends in DDoS Attacks

*17 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.

*18 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.

*19 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.

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

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the Malware Investigation Task Force (MITF)*[21], a malware activity observation project operated by IIJ. The MITF uses honeypots*[22] connected to the Internet in a manner similar to general users in order to observe communications arriving over the Internet. Most appear to be communications by malware selecting a target at random, or scans attempting to locate a target for attack.

■ Status of Random Communications

Figure 3 shows trends in the total volumes of communications coming into the honeypots (incoming packets) between October 1 and December 31, 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 scanning behavior targeting TCP ports utilized by Microsoft operating systems. As with the prior study, we observed scanning behavior for 2967/TCP used by Symantec client software and 4899/TCP used by PC remote management tools. At the same time, communications for which the goal was not clearly identifiable, such as 2582/TCP and 31138/TCP (not used by general applications), were also observed. Looking at the overall sender distribution by country, we see that attacks sourced to China and Japan, 22.6% and 20.0%, respectively, were comparatively higher than the rest.

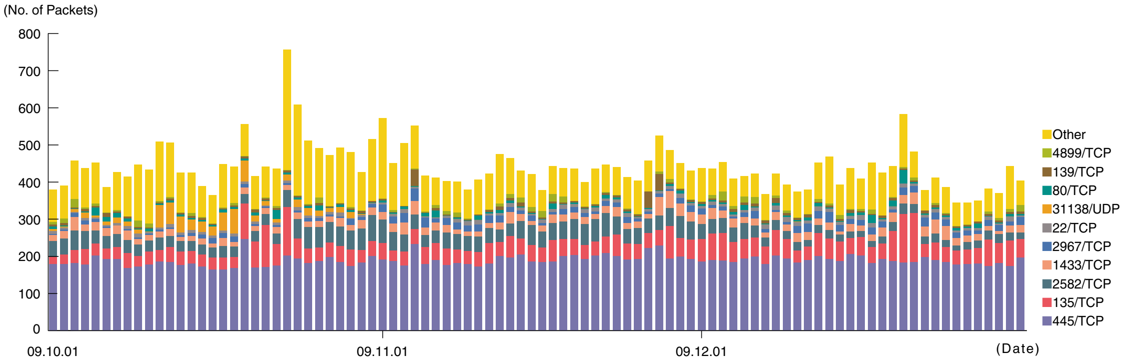


Figure 3: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

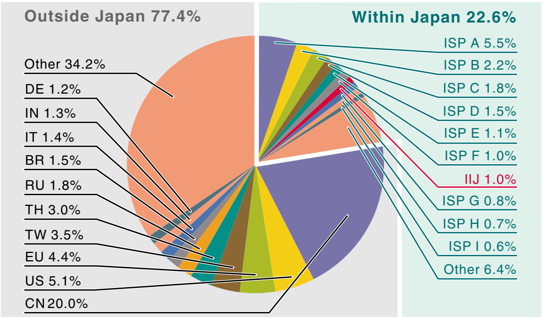


Figure 4: Sender Distribution (by Country, Entire Period under Study)

[21] Malware Investigation Task Force (MITF). The MITF began activities in May 2007, observing malware network activity through the use of honeypots to gauge trends and gather technical information, and attempting to link these findings to the creation of countermeasures.

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

Malware Network Activity

Next, we will take a look into the malware activity observed by the MITF. Figure 5 shows trends in the total number of malware specimens acquired during the period under study. Figure 6 shows the distribution of the specimen acquisition source for malware. In Figure 5, the trends in the number of acquired specimens show the total number of specimens acquired per day*[23], while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*[24].

On average, 623 specimens were acquired per day during the period under study, representing about 44 different malware variants. According to the statistics in our prior whitepaper, the average daily total for acquired specimens was 592, with 46 different variants. This indicates that both the number of specimens and the number of unique variants for this period were about the same as for the previous period.

The distribution of specimens according to source country has Japan at 60.2%, with other countries accounting for the 39.8% balance. Of the total, malware infection activity among IIJ users was 3.0%, maintaining a low value similar to the previous period.

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, 4.3% of the malware specimens were worms, 93.1% were bots, and 2.6% were downloaders. In addition, the MITF confirmed the presence of 42 botnet C&C servers*[25] and 519 malware distribution sites.

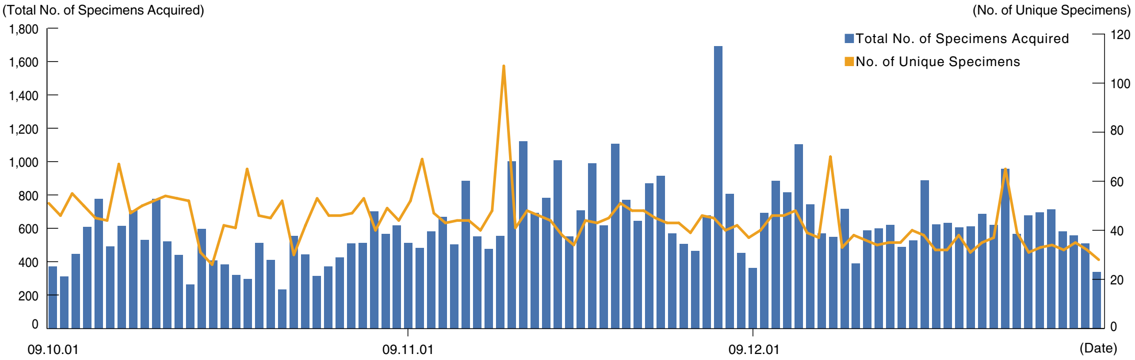


Figure 5: Trends in the Number of Malware Specimens Acquired (Total Number, Number of Unique Specimens)

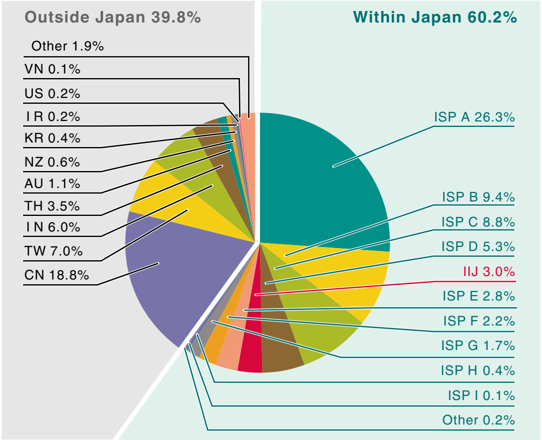


Figure 6: Distribution of Acquired Specimens by Source (by Country, Entire Period under Study)

*23 This indicates the malware acquired by honeypots.

*24 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.

*25 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*[26]. 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 October 1 and December 31, 2009. Figure 8 shows the distribution of attacks according to source. These are a summary of attacks detected by signatures on the IIJ Managed IPS Service. Japan was the source for 61.7% of attacks observed, while China and the United States accounted for 6.7% and 5.3%, respectively, with other countries following in order.

We noted the number of SQL injection attacks on Web servers similar to our prior whitepaper. Sporadic rises in attacks are those detected at multiple targets from a specific attack source.

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

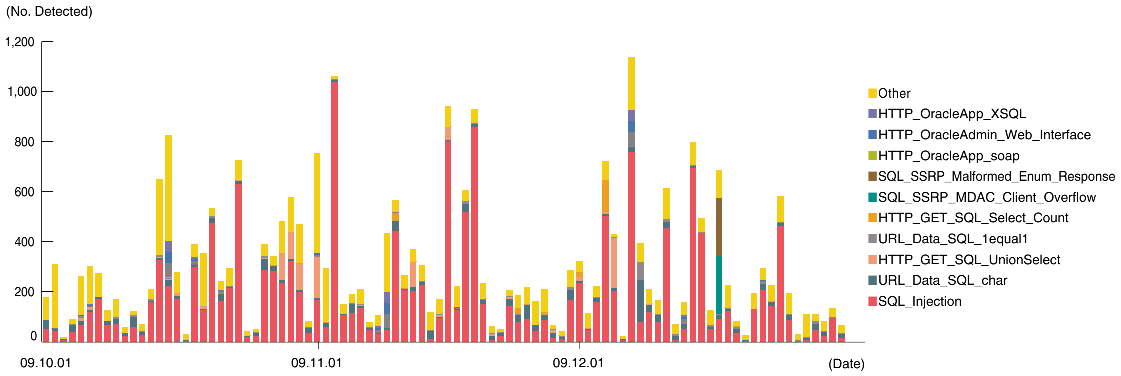


Figure 7: Trends in SQL Injection Attacks (by Day, by Attack Type)

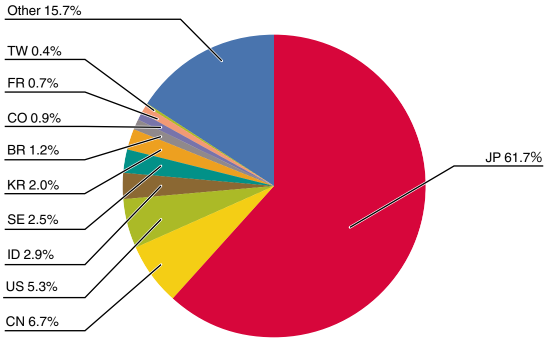


Figure 8: Distribution of SQL Injection Attacks by Source (by Country, Entire Period under Study)

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

1.4 Focused Research

Incidents occurring over the Internet change in type and scope almost from one minute to the next. Accordingly, IIJ works toward taking countermeasures by performing independent surveys and analyses. Here we will present information from the surveys we have undertaken during this period regarding the renewed Gumblar activity, MITM attacks using a vulnerability in the renegotiation feature of SSL and TLS, and techniques for observing P2P file sharing networks.

1.4.1 Renewed Gumblar Activity

The Gumblar malware that was active from April 2009 began renewed activity in October 2009 and continued spreading through December, causing further damage. Here we will explain the situation by focusing on differences between recent incidents and the previous Gumblar*[27].

■ The New Gumblar

Gumblar is a malware infection incident originating through Web content that was altered using FTP accounts that were stolen in advance. IDs and passwords on infected machines are stolen by the malware and used to perpetrate further alterations, broadening the scope of damages. This is a complex incident involving multiple websites and pieces of malware*[28]. The current propagation has been noticed from the alteration of a number of websites that took place around October 12*[29], and infections continue to occur as of the time of writing.

As with the previous incident, the new Gumblar also induces infection via multiple websites. Previously a small number of servers were used as dedicated malware distribution sites, but for the current incident a large number of altered websites are being exploited. For this reason, it is difficult to stop the spread of the current incident by prohibiting access to or taking down malware distribution sites (Figure 9).

The total numbers of altered websites and stolen IDs and passwords are not known, but several pieces of information that have been published indicate the scale of this activity. For example, there are reports that approximately 80,000 websites have been altered to induce malware infections (over 3,000 in Japan), and that over 2,000 malware distribution sites have existed (approximately 80 in Japan)*[30].

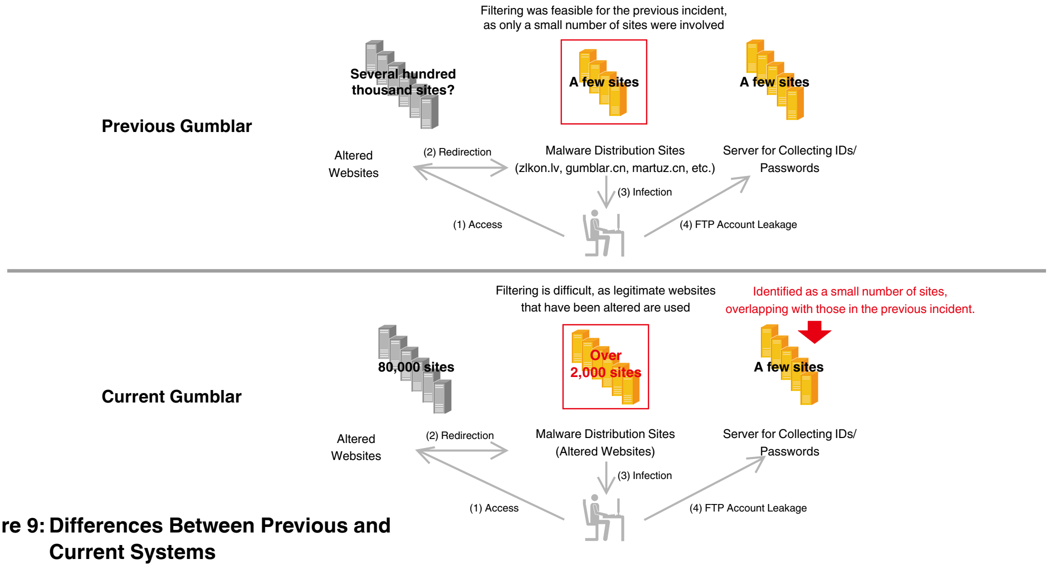

Filtering was feasible for the previous incident, as only a small number of sites were involved
Several hundred thousand sites?
A few sites
A few sites
Previous Gumblar
Altered Websites
(2) Redirection
Malware Distribution Sites (zlkon.lv, gumblar.cn, martuz.cn, etc.)
Server for Collecting IDs/ Passwords
(3) Infection
(1) Access
(4) FTP Account Leakage
Filtering is difficult, as legitimate websites that have been altered are used
Identified as a small number of sites, overlapping with those in the previous incident.
80,000 sites
Over 2,000 sites
A few sites
Current Gumblar
Altered Websites
(2) Redirection
Malware Distribution Sites (Altered Websites)
Server for Collecting IDs/ Passwords
(3) Infection
(1) Access
(4) FTP Account Leakage

Figure 9: Differences Between Previous and Current Systems

[27] Gumblar was a portion of the name of a malware distribution website (gumblar.cn) that was used between April and May, 2009. In this whitepaper we use the name Gumblar to refer to all related websites and malware. The name Gumblar.X is also commonly used to differentiate between the current incident and the previous one.

[28] See IIR Vol.4, "ID/Password Stealing Gumblar Malware" for more information about the incident that occurred from April, such as the role of websites in Gumblar, and an analysis of the behavior of the malware (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol04_EN.pdf).

[29] The cNotes reported that attacks were first observed on October 12. "The second coming of zlkon, gumblar, and martuz" (http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=zlkon%A1%A2gumblar%A1%A2martuz+%BA%C6%CE%D7) (in Japanese).

[30] Site numbers in this article were sourced from the "Gumblar infection count" entry of the Analyst's Diary on the following Kaspersky Labs blog (http://www.viruslist.com/en/weblog?weblogid=208187923).

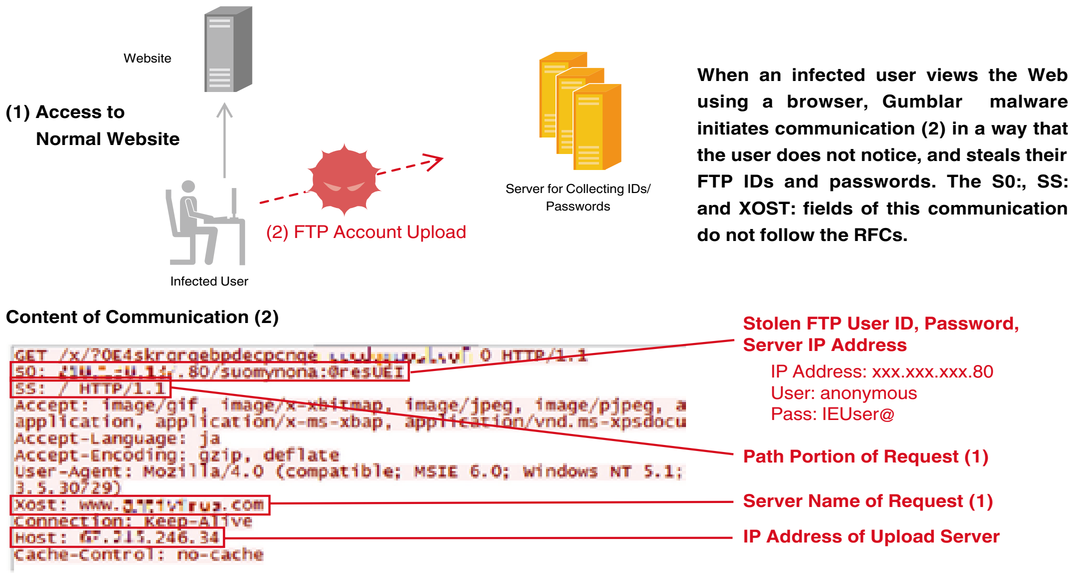
Currently Used Malware and Countermeasures

IIJ has analyzed multiple specimens of malware used in the current incident. As a result, we have confirmed that varieties with several additional functions compared to the previous malware are being used*[31]. As with the previous incident, the transmission of stolen IDs and passwords to servers is still being carried out. A distinctive header that does not follow the RFCs and is not found in normal HTTP requests is used for this communication. This means that by monitoring communications using proxy servers or Intrusion Detection Systems it is possible to identify infected users and prevent the leakage of IDs and passwords (Figure 10). Because it has been established that like the previous incident stolen IDs and passwords are only uploaded to a small number of servers, we attempted to take down*[32] these servers. However, we confirmed that the malware quickly switched to other servers and resumed its activity.

More Recent Incidents

In parallel with this, incidents using completely different altered content and infection methods, as well as new malware and communication methods, began occurring from the beginning of December*[33]. These utilized more advanced malware infection methods, and exploited a vulnerability in the Java Runtime Environment*[34] and a new vulnerability in Adobe Reader (including Acrobat)*[35]. It has been confirmed that the malware that infected users steals IDs and passwords from FTP client settings and demonstrates bot-like behavior. This incident involves the alteration of a large number of websites between late 2009 and early 2010.

As demonstrated above Gumblar is still a current incident, so care must continue to be taken with regard to managing client OS and software versions, managing passwords, and being on the lookout for Web content alterations.


Website
(1) Access to Normal Website
(2) FTP Account Upload
Server for Collecting IDs/ Passwords
Infected User
Content of Communication (2)
Stolen FTP User ID, Password, Server IP Address
IP Address: xxx.xxx.xxx.80
User: anonymous
Pass: IEUser@
Path Portion of Request (1)
Server Name of Request (1)
IP Address of Upload Server

When an infected user views the Web using a browser, Gumblar malware initiates communication (2) in a way that the user does not notice, and steals their FTP IDs and passwords. The S0:, SS: and XOST: fields of this communication do not follow the RFCs.

```
GET /x/?OE4skrorgebpdecpcnge [redacted] 0 HTTP/1.1
S0: [redacted].80/suomynona:0resUEI
SS: / HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, a
application, application/x-ms-xbap, application/vnd.ms-xpsdocu
Accept-Language: ja
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;
3.5.30729)
Xost: www.[redacted]rus.com
Connection: Keep-Alive
Host: [redacted].246.34
Cache-Control: no-cache
```

Figure 10: Communication of Gumblar Stealing FTP Account

[31] For example registry concealment, blocking access to specific websites, and preventing the startup of rootkit detection tools. Rootkits are tools that were originally used to gain root access to UNIX systems. They were often used in tandem with tools that concealed this behavior, and rootkit became a general term for tools that usurp privileges and conceal what is taking place. Because Gumblar behaves like a rootkit, using API hooking and the concealment of certain registry entries to steal IDs and passwords, it attempts to prevent itself from being detected by rootkit detection tools.

[32] IIJ issued take-down requests to JPCERT/CC for the servers it confirmed. It is possible to submit take-down requests for servers like this that are used for malicious activities by issuing an incident report notification (http://www.jpcert.or.jp/english/ir/form.html).

[33] Due to differences in the alterations that induce malware infection and the malware that is used, this incident is sometimes not referred to as Gumblar. It is known variously as GNU GPL (CODE1, LGPL), ru:8080, and 8080 due to the nature of the alterations.

[34] The fact that a vulnerability in the Java Runtime Environment (JRE) is being used has been reported in the IBM ISS Tokyo SOC Report (http://www-935.ibm.com/services/jp/index.wss/consultantpov/secpriv/b1333966?cntxt=a1010214) (in Japanese).

[35] The fact that a vulnerability in Adobe Acrobat and Adobe Reader is being used has also been reported in the IBM ISS Tokyo SOC Report (http://www-935.ibm.com/services/jp/index.wss/consultantpov/secpriv/b1333971?cntxt=a1010214) (in Japanese). A patch had not been released for this vulnerability at the time it was exploited, making this a 0-day attack. At the time of writing this issue has been addressed in "Security updates available for Adobe Reader and Acrobat" (http://www.adobe.com/support/security/bulletins/apsb10-02.html).

1.4.2 MITM Attacks Using a Vulnerability in the SSL and TLS Renegotiation

■ Background

In November 2009, Marsh Ray, Steve Dispensa and Martin Rex released details of a vulnerability[36] in the SSL and TLS protocols[37][38] that could allow Man-in-the-Middle attacks[39] to be carried out. SSL and TLS operate between the IP and application layers and ensure confidentiality and integrity for application data, authenticating the target of communications using X.509 public key certificates. As they are used together with application layer communication protocols such as HTTP, SMTP, and POP, this vulnerability affects a large number of applications and systems.

In particular, the HTTPS (HTTP over SSL) protocol[40] is implemented in a large number of Web browsers and Web servers, and Marsh Ray et al. gave an example of an attack method using HTTPS in the report. It has also been established that the vulnerability is exploitable through the release of methods for posting password information to an attacker's Twitter account by applying the vulnerability to the Twitter API[41]. Thierry Zoller investigated whether or not the vulnerability could be applied to protocols other than HTTP[42]. In his report, he showed that FTPS and SMTPS are vulnerable, and EAPTLS is not affected, but there are still application protocols for which the impact is not yet clear, such as POP and LDAP.

This vulnerability can be attributed to a problem in the SSL and TLS protocol specifications themselves. Fixes have been released for OpenSSL[43] and Apache[44], but most of these involve simply disabling the renegotiation feature that is causing the problem[45]. More thorough measures would require an update to the current specifications and migration to implementations that follow the new specifications. The IETF[46] has been in the same line and an RFC that establishes countermeasures was published with unprecedented speed (RFC5746[47]). This vulnerability affects all versions of the TLS protocol, in addition to SSL version 3.0. SSL specifications are not under IETF change control, but the RFC indicates that the TLS solution can also be applied to SSL (RFC5746 section 4.5).

■ MITM Attacks Exploiting the Renegotiation

In SSL and TLS, a client and server negotiate encryption algorithm and key information by handshake protocol before the sending and receiving of application data is carried out safely. The renegotiation feature is used to update algorithm and key information that has been accepted by both client and server. The vulnerability report indicated that when an issue in the renegotiation specifications is exploited, it is possible to intercept SSL and TLS communications using a Man-in-the-Middle attack. A specific example that was pointed out was a situation where mutual authentication (with client authentication using a public key certificate) is switched from server authentication during a session.

[36] Marsh Ray, Steve Dispensa, "Renegotiating TLS" (http://extendedsubset.com/Renegotiating_TLS.pdf).
This vulnerability is managed as CVE-2009-3555 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555) and Vulnerability Note VU#120541, "SSL and TLS Protocols renegotiation vulnerability" (http://www.kb.cert.org/vuls/id/120541).

[37] Alan O. Freier, Philip Karlton, Paul C. Kocher, Internet Draft "The SSL Protocol Version 3.0" (http://tools.ietf.org/html/draft-ietf-tls-ssl-version3-00).

[38] Dierks, T. and E. Rescorla, RFC 5246 "The Transport Layer Security (TLS) Protocol Version 1.2" (http://www.ietf.org/rfc/rfc5246.txt).

[39] Man-in-the-Middle attacks are those targeted at communications where the attacker is positioned between the two parties carrying out communications. This can result in communications being intercepted or altered (including cases where the attacker poses to each party as the other). When evaluating whether or not this attack method can succeed and investigating countermeasures, it is assumed that there is an attacker in the middle during communications. In order for a Man-in-the-Middle attack to succeed in practice, it must be used in combination with other methods for intercepting communications (for example, route hijacking over the Internet).

[40] E. Rescorla, "HTTP Over TLS" (http://www.ietf.org/rfc/rfc2818.txt).

[41] Anil Kurmus's blog identifies the Twitter API issues "TLS renegotiation vulnerability (CVE-2009-3555)" (http://www.securegoose.org/2009/11/tls-renegotiation-vulnerability-cve.html). The issues identified here were quickly fixed by Twitter.

[42] Thierry Zoller, "TLS & SSLv3 renegotiation vulnerability" (http://www.g-sec.lu/practicaltls.pdf).

[43] OpenSSL Security Advisory (http://www.openssl.org/news/secadv_20091111.txt). During proofreading, the OpenSSL project team announced the release of version 0.9.8m which implements RFC5746 (http://cvs.openssl.org/getfile?f=openssl/CHANGES&v=OpenSSL_0_9_8m).

[44] http://www.apache.org/dist/httpd/patches/apply_to_2.2.14/CVE-2009-3555-2.2.patch
During proofreading, the Apache HTTP server project team announced the release of version 2.2.15 corresponding to OpenSSL 0.9.8m which implements RFC5746 (http://www.apache.org/dist/httpd/CHANGES_2.2.15).

[45] It is possible to confirm whether or not renegotiation is enabled using the following TLS Renegotiation Test. "TLS Renegotiation Test" (http://netsekure.org/2009/11/tls-renegotiation-test/).

[46] Internet Engineering Task Force. The organization that develops Internet technical standards such as communication protocols and data formats. They issue the Request for Comments (RFC) documents that regulate standard specifications. Draft RFC documents are known as Internet drafts.

[47] E. Rescorla, M. Ray, S. Dispensa, N. Oskov, RFC5746, "Transport Layer Security (TLS) Renegotiation Indication Extension" (http://www.ietf.org/rfc/rfc5746.txt). The Internet draft this RFC is based on was proposed in November 2009, discussed quickly for the relatively short period of three months, and made an RFC in February 2010.

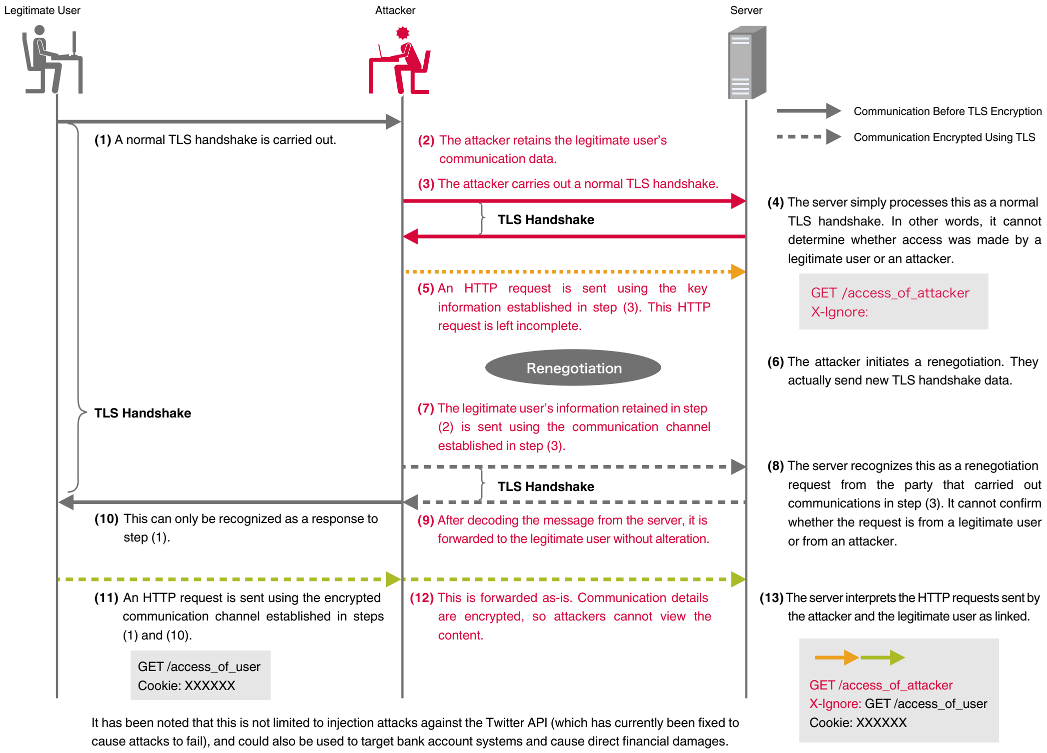
Figure 11 shows an example of an attack using HTTPS. This attack allows attackers as the man-in-the-middle to interrupt encrypted communications between a client and server. As a result, attackers are able to combine their HTTP requests with those of a legitimate user, and send them to the server. Note that at this point the legitimate user's application data is still encrypted, and no alteration or eavesdropping by an attacker will take place. When attackers' requests are linked with a legitimate user's existing requests using an HTTP cookie, servers will interpret the linked requests as both having come from the same user, so there is a chance that an attacker's requests will be accepted and processed.

■ RFC Modifications

Next, we will explain the modifications in the new RFC. This RFC introduces a new "renegotiation_info" TLS extension value, in addition to a "TLS_EMPTY_RENEGOTIATION_INFO_SCSV" state for the cipher suite that normally defines the encryption algorithm. Using the renegotiation_info extension, it is possible to announce to a target of communications that the current implementation can safely carry out renegotiation. More specifically, the client and server both save information shared safely by handshake protocol. When carrying out renegotiation information that cannot be known to outside parties is exchanged using the renegotiation_info extension to confirm that each party is the same as when communication began. Additionally, because some implementations detect the renegotiation_info extension as a TLS extension that cannot be processed and terminate communication, a method utilizing "TLS_EMPTY_RENEGOTIATION_INFO_SCSV" has also been made available.

■ Countermeasures and Backward Compatibility Issues

The current issue will be resolved when implementations compliant with the RFC5746 countermeasures spread, but migration is expected to take some time. From a backward compatibility perspective it is important to maintain compatibility with the current version, but when renegotiation is carried out using a previous implementation, there is no safe way of confirming that a request is coming from a legitimate party. For this reason, it is recommended that renegotiation requests from previous implementations are rejected in new implementations. This is in effect the same as the current temporary countermeasure that does not allow use of the renegotiation. In other words, when renegotiation must be carried out safely, a new implementation that supports the new specifications must be deployed for both client and server.



(1) A normal TLS handshake is carried out.

(2) The attacker retains the legitimate user's communication data.

(3) The attacker carries out a normal TLS handshake.

(4) The server simply processes this as a normal TLS handshake. In other words, it cannot determine whether access was made by a legitimate user or an attacker.

GET /access_of_attacker
X-Ignore:

(5) An HTTP request is sent using the key information established in step (3). This HTTP request is left incomplete.

(6) The attacker initiates a renegotiation. They actually send new TLS handshake data.

(7) The legitimate user's information retained in step (2) is sent using the communication channel established in step (3).

(8) The server recognizes this as a renegotiation request from the party that carried out communications in step (3). It cannot confirm whether the request is from a legitimate user or from an attacker.

(9) After decoding the message from the server, it is forwarded to the legitimate user without alteration.

(10) This can only be recognized as a response to step (1).

(11) An HTTP request is sent using the encrypted communication channel established in steps (1) and (10).

GET /access_of_user
Cookie: XXXXXX

(12) This is forwarded as-is. Communication details are encrypted, so attackers cannot view the content.

(13) The server interprets the HTTP requests sent by the attacker and the legitimate user as linked.

GET /access_of_attacker
X-Ignore: GET /access_of_user
Cookie: XXXXXX

It has been noted that this is not limited to injection attacks against the Twitter API (which has currently been fixed to cause attacks to fail), and could also be used to target bank account systems and cause direct financial damages.

Figure 11: Attack Scenario

1.4.3 Techniques for Surveying P2P File Sharing Networks

■ Introduction

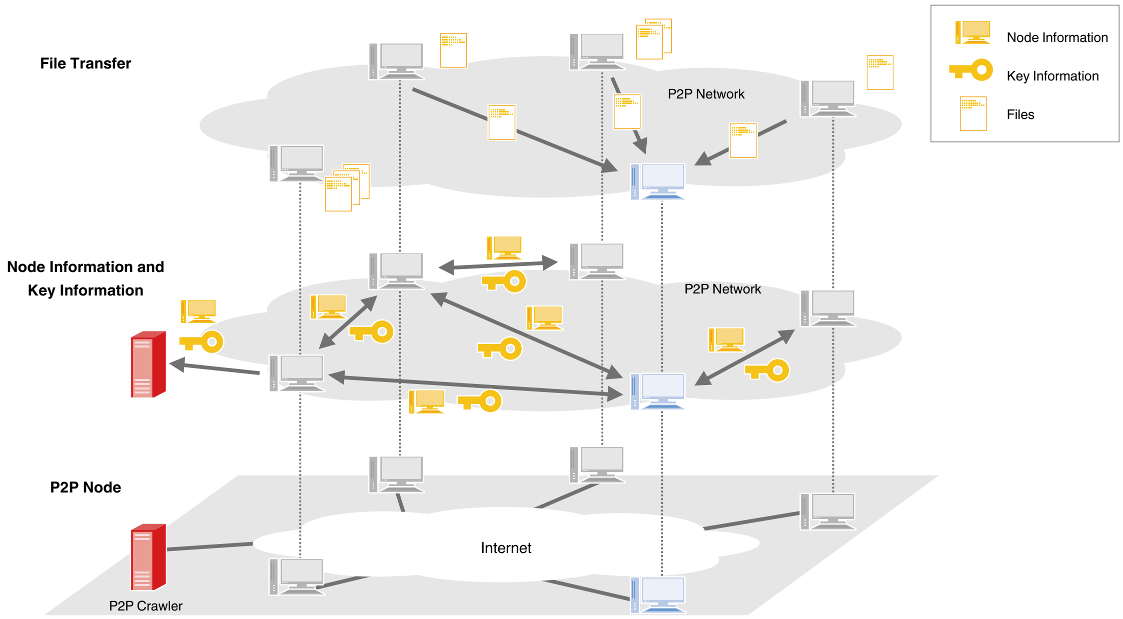
IIJ observes techniques for surveying P2P networks formed using P2P file sharing software such as Winny and Share (two of the implementations popular in Japan) from the dual perspectives of considering countermeasures to prevent information leakage and investigating the characteristics of communication volume, and has been actively participating in related research projects*[48] since 2006.

P2P file sharing networks are once again drawing attention for the connection they have with copyright infringement due to the inclusion of a provision making the download of illegally copied material illegal in the amended Copyright Act*[49] that came into effect on January 1, 2010. Here we take this opportunity to summarize P2P file sharing network systems such as Winny and Share, as well as techniques for surveying such networks.

■ P2P File Sharing Network Systems

P2P file sharing networks have functions for making files publicly available in order to share them, functions for searching for files, and functions for downloading files. P2P nodes exchange “key information” that indicates which nodes have which files in order to search for the desired files more efficiently. This key information exchange system is also used for notifying other nodes of the files that are made available.

One of the methods used to increase the overall download efficiency of a P2P file sharing network is the caching of files that have been downloaded, which are automatically made available to other nodes. They also feature systems where even if a user has not downloaded a file themselves, a cache is automatically created through a file transfer relay. Through this system popular files are automatically made available on large numbers of nodes. Under a pure P2P system, a P2P file sharing network is sustained through the process of nodes exchanging information on other nodes and accumulating it to allow unknown numbers of nodes to participate in and withdraw from the network freely. Figure 12 shows a summary of this explanation. Actual P2P file sharing software collects files automatically based on keywords that users specify. This means that key information collection and file transfer communications can occur constantly on P2P file sharing networks, increasing traffic volumes.



P2P nodes connected to the Internet (lower layer) form a P2P network by connecting with other nodes, exchanging and accumulating node information and key information (middle layer). Nodes that wish to download a file (the blue node) search for it using the accumulated key information, identify nodes that have that file (or a portion of it), and then connect directly to those nodes to request the transfer of the file (upper layer). On the other hand, P2P crawlers only connect to nodes and collect node information and key information (lower to middle layers), and do not transfer files.

Figure 12: P2P File Sharing Network Systems

*48 For example, the Secure Trusted Network Forum's P2P research group (http://www.scat.or.jp/stnf/) (in Japanese).

*49 The provisions of the Copyright Act can be viewed using the Japanese Law Translation (http://www.japaneselawtranslation.go.jp/?re=02).

■ Techniques for Surveying P2P File Sharing Networks

On P2P networks, there is no server which maintains centralized information on the whole network. For this reason, crawling methods are used to get an overall picture of a network*[50]. When carrying out a crawling survey, crawlers connect with P2P nodes and communicate using the protocol of the P2P file sharing network to acquire information about other nodes. Then, crawlers connect with the nodes that were newly discovered, and repeat the process of acquiring information about other nodes, comprehensively surveying the nodes on a P2P file sharing network (Figure 13).

By analyzing the key information that is collected along with the node information during a crawling survey, it is also possible to ascertain what kinds of files are being made public at which nodes. Surveys using this kind of crawling method have the advantage of giving an overall picture of a P2P file sharing network without side effects such as the dissemination of files.

■ The Current State of P2P Networks

We will present a portion of the results from surveys that IIJ is carrying out in cooperation with an external organization as an example of surveys of the current state of P2P file sharing networks*[51]. Through these surveys we have learned that approximately 2% of all Winny nodes and 3% of all Share nodes exist on the IIJ network. We are also evaluating the impact that this has on the entire network by ascertaining the amount of traffic that is generated by these nodes through communications with nodes outside the IIJ network. Figure 14 shows changes in the number of Winny and Share nodes*[52] that were identified through these surveys, and Figure 15 shows the results of surveying the traffic generated by nodes on the IIJ network through communication with nodes outside the IIJ network.

The results show that the number of nodes for both Winny and Share is in a downward trend, but they still occupy approximately 6Gbps of bandwidth on a constant basis at this point in time.

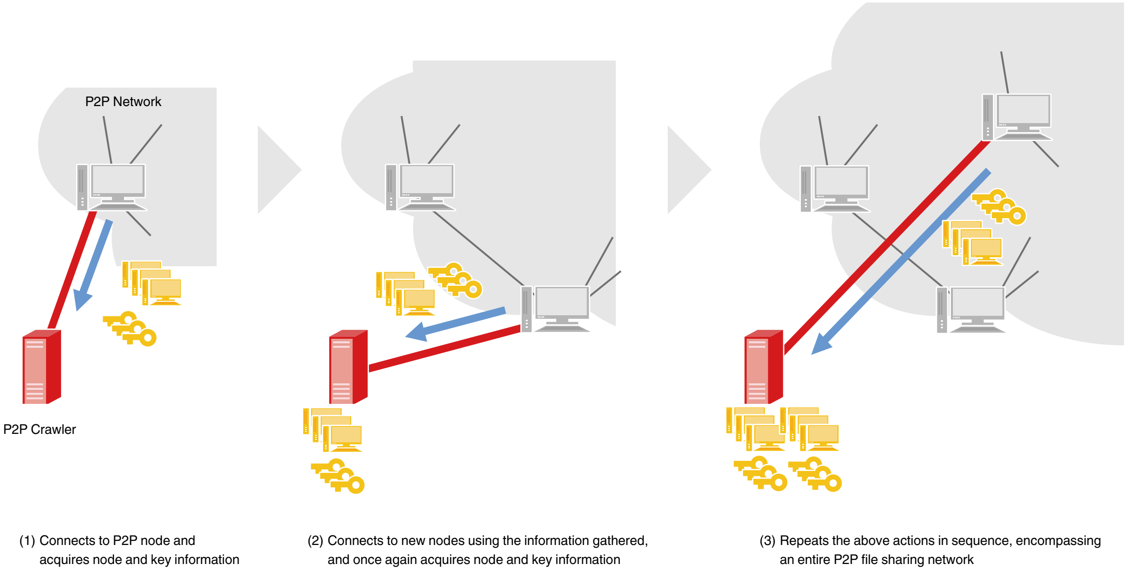

P2P Network
P2P Crawler
(1) Connects to P2P node and acquires node and key information
(2) Connects to new nodes using the information gathered, and once again acquires node and key information
(3) Repeats the above actions in sequence, encompassing an entire P2P file sharing network

Figure 13: Crawling Method Overview

*[50] Crawling survey reports are also given in the following paper. Terada et al., “P2P network observation using crawling method”, Information Processing Society of Japan Computer Security Group Report Vol. 2007, No. 48, pp. 51-56 (2007) (http://jvnrss.ise.chuo-u.ac.jp/jtg/doc/CSEC07037009.pdf) (in Japanese). Winny Radar and Share Radar of Fourteenforty Research Institute, Inc. (http://www.fourteenforty.jp/) (in Japanese) are examples of products that conduct surveys like this.

*[51] Surveys of the current state of P2P file sharing networks include “The Current State of P2P - Winny and Share Network Status Survey Report -” conducted by CROSSWARP Inc. (http://www.scat.or.jp/stnf/contents/p2p/p2p080910_2.pdf) (in Japanese). Several other surveys of the current state of affairs were presented at the Information Security Seminar hosted by the Secure Trusted Network Forum in September 2008, and the materials presented can be downloaded from their website (http://www.scat.or.jp/stnf/contents/p2p080910.html) (in Japanese). The next seminar was held on March 2, 2010 (http://www.scat.or.jp/stnf/contents/p2p100302/P2P.htm) (in Japanese).

*[52] About the time that the amended Copyright Act came into effect on January 1, 2010, a drop in node numbers for both Winny and Share of about 20% was observed. Note that the node numbers shown in this figure are values for after the drop occurred.

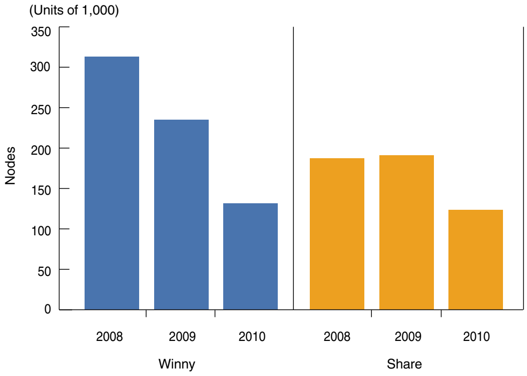
Here we presented the current state of Winny and Share, which we are surveying on a regular basis. Other P2P file sharing network implementations exist, and there is a possibility that communication characteristics may continue to evolve drastically due to changing user habits. IIJ will continue to carry out surveys like this in order to keep providing a stable network infrastructure.

1.5 Conclusion

This whitepaper has provided a summary of security incidents to which IIJ has responded.

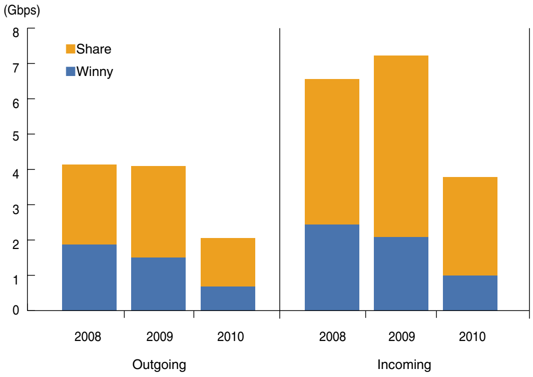
In this volume we provided a follow-up on the continuing Gumblar incidents, and summarized vulnerabilities in the SSL and TLS communications protocols, as well as techniques for surveying P2P file sharing networks. P2P file sharing networks are not a particularly new subject, being a topic that has sparked a variety of debates, such as the volume of traffic they generate, their anonymity, information leakages, and copyright infringement, and IIJ has been surveying them over an extended period. In this volume we have only covered a few topics, such as survey methods and impact on traffic volumes, but we would like to continue surveying these networks and examine different facets of them when the opportunity arises.

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.



The survey was conducted over one week in January of each year. Nodes were counted every 24 hours after removing duplicates to gain a daily number of nodes, and the average of this figure over 7 days was used as the number of nodes for that year.

Figure 14: Comparison of Average Daily Nodes for Winny and Share



Average traffic was calculated for one week (the same week as Figure 14) in January of each year. Outgoing traffic refers to traffic from inside the IIJ network going to external networks, and incoming traffic refers to traffic from outside the IIJ network coming in.

Figure 15: Winny and Share Traffic (Temporal Average for 1 Week)

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 Renewed Gumblar Activity)
Yuji Suga (1.4.2 MITM Attacks Using a Vulnerability in the SSL and TLS Renegotiation)
Mamoru Saito, Tadaaki Nagao (1.4.3 Techniques for Surveying P2P File Sharing Networks)
Division of Emergency Response and Clearinghouse for Security Information, IIJ Service Business Department

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