Malware Infections Resulting from Mashup Content

In this report, we will explain incidents that occurred between October and December 2010, and discuss a series of DDoS attacks that took place in September 2010, malware infections resulting from mashup content, alterations of software distribution packages, and the anti-Malware engineering WorkShop 2010.

1.1 Introduction

This report summarizes incidents to which IIJ responded, based on general information obtained by IIJ itself related to the stable operation of the Internet, information from observations of incidents, information acquired through our services, and information obtained from companies and organizations with which IIJ has cooperative relationships. This volume covers the period of time from October 1 through December 31, 2010. In this period a number of vulnerabilities related to Web browsers and their plug-ins continued to be exploited, and mobile phone vulnerabilities and their exploitation became a real threat. Incidents in which SIP was exploited leading to financial damages have also been occurring on an ongoing basis. Multiple large-scale DDoS attacks took place internationally. Additionally, whistle-blowing activities and information leaks such as those carried out by WikiLeaks became a major topic of discussion. 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, 2010. Figure 1 shows the distribution of incidents handled during this period*1.

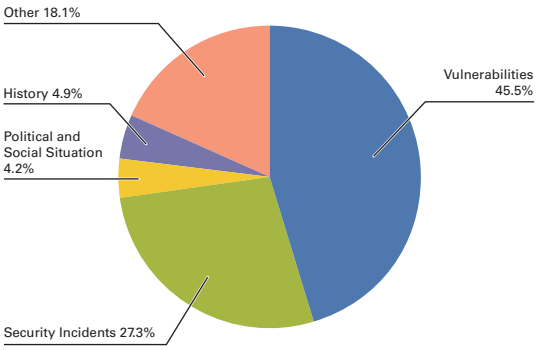


Figure 1: Incident Ratio by Category (October 1 to December 31, 2010)

■ Vulnerabilities

During this period a large number of vulnerabilities were discovered and fixed in Web browsers and applications such as Microsoft's Windows*2*3*4, Internet Explorer*5, and Office products*6, Adobe Systems' Adobe Reader and Acrobat*7, Flash Player*8, and Shockwave Player*9, Apple's QuickTime*10, and Oracle's JRE*11. Several of these vulnerabilities were exploited before patches were released. Vulnerabilities were also patched in other widely-used software, including server applications such as Oracle's Oracle Database*12, BIND DNS servers*13, ISC DHCP servers*14, Adobe Flash Media Server*15, the CMS*16 platform WordPress*17, and the blog software Movable Type*18, as well as the glibc*19*20 library used in UNIX-based OSes, and the VMware*21 virtualization software. During this

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

*2 Microsoft Security Bulletin MS10-070 - Important: Vulnerability in ASP.NET Could Allow Information Disclosure (2418042) (http://www.microsoft.com/technet/security/bulletin/ms10-070.mspx).

*3 Microsoft Security Bulletin MS10-091 - Critical: Vulnerabilities in the OpenType Font (OTF) Driver Could Allow Remote Code Execution (2296199) (http://www.microsoft.com/technet/security/bulletin/ms10-091.mspx).

*4 Microsoft Security Bulletin MS10-092 - Important: Vulnerability in Task Scheduler Could Allow Elevation of Privilege (2305420) (http://www.microsoft.com/technet/security/bulletin/ms10-092.mspx).

*5 Microsoft Security Bulletin MS10-090 - Critical: Cumulative Security Update for Internet Explorer (2416400) (http://www.microsoft.com/technet/security/bulletin/ms10-090.mspx).

period multiple vulnerabilities were also patched in mobile phone firmware and applications such as Apple's iOS*22 and Flash Player*23 for Android phones.

■ Political and Social Situations

IIJ pays close attention to various political and social situations related to international affairs and current events. During this period we turned our attention to the selection of Nobel Peace Prize awardees, APEC Japan 2010 held in Yokohama*24, and North Korea's shelling of South Korea, but we noted no related Internet attacks.

■ History

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

■ Security Incidents

Unanticipated security incidents not related to political or social situations occurred in the form of malware infections via a Web analytics service*25*26. See "1.4.2 Malware Infections Resulting from Mashup Content" for more information about these incidents. The unauthorized SIP communications that have been occurring in the past also continued*27, and a warning about its exploitation for malicious purposes was released*28. There were also continued attempts to exploit social network services such as Twitter and Facebook*29 to obtain information or infect users with malware*30. During this period there were also multiple large-scale DDoS attacks, including attacks relating to elections in Burma*31, and others connected to WikiLeaks*32 and the U.S. holiday shopping season*33.

*6 Microsoft Security Bulletin MS10-087 - Critical: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2423930) (http://www.microsoft.com/technet/security/bulletin/ms10-087.mspx).
*7 APSB10-28 Security updates available for Adobe Reader and Acrobat (http://www.adobe.com/support/security/bulletins/apsb10-28.html).
*8 APSB10-26 Security update available for Adobe Flash Player (http://www.adobe.com/support/security/bulletins/apsb10-26.html).
*9 APSB10-25 Security update available for Shockwave Player (http://www.adobe.com/support/security/bulletins/apsb10-25.html).
*10 About the security content of QuickTime 7.6.9 (http://support.apple.com/kb/HT4447).
*11 Oracle Corporation, "Java Platform, Standard Edition 6 Update Release Notes" (http://www.oracle.com/technetwork/java/javase/6u22releasenotes-176121.html).
*12 Oracle Corporation, "Oracle Critical Patch Update Advisory - October 2010" (http://www.oracle.com/technetwork/topics/security/cpuoct2010-175626.html).
*13 BIND: cache incorrectly allows a ncache entry and a rrsig for the same type (http://www.isc.org/software/bind/advisories/cve-2010-3613).
*14 DHCP: Server Hangs with TCP to Failover Peer Port (http://www.isc.org/software/dhcp/advisories/cve-2010-3616).
*15 APSB10-27 Security update available for Adobe Flash Media Server (http://www.adobe.com/support/security/bulletins/apsb10-27.html).
*16 CMS is an abbreviation of Content Management System. These are used to manage websites and portal sites.
*17 WordPress 3.0.2 (http://wordpress.org/news/2010/11/wordpress-3-0-2/), WordPress 3.0.3 (http://wordpress.org/news/2010/12/wordpress-3-0-3/), 3.0.4 Important Security Update (http://wordpress.org/news/2010/12/3-0-4-update/).
*18 Movable Type 5.04 and 4.35 Security Update (http://www.movabletype.com/blog/2010/12/movable-type-504-and-435-security-update.html).
*19 Vulnerability Note VU#537223 GNU C library dynamic linker expands $ORIGIN in setuid library search path (http://www.kb.cert.org/vuls/ id/537223).
*20 CVE-2010-3856 glibc: ld.so arbitrary DSO loading via LD_AUDIT in setuid/setgid programs (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-3856).
*21 VMware hosted products and ESX patches resolve multiple security issues (http://www.vmware.com/security/advisories/VMSA-2010-0018.html).
*22 About the security content of iOS 4.2 (http://support.apple.com/kb/HT4456).
*23 Security update APSB10-26 detailed in footnote *8 includes details of the update to Flash Player for Android.
*24 Asia-Pacific Economic Cooperation: APEC (http://www.mofa.go.jp/policy/economy/apec/2010/).
*25 JPCERT Coordination Center, "Web analytics service exploited for malicious purposes" (http://www.jpcert.or.jp/english/at/2010/at100028.txt).
*26 Details can be found in the following Trend Micro security blog post. "Aimed at financial gain through affiliates!? - a follow-up report on 'mstmp' and 'lib.dll' attacks" (http://blog.trendmicro.co.jp/archives/3728) (in Japanese).
*27 cNotes provides SIP observation data on an irregular basis. For example, the IP addresses of attackers and lists of the IDs used in brute force attacks. Fraudulent incoming SIP 32 (http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=%C9%D4%C0%B5%A4%CASIP%C3%E5%BF%AE+32) (in Japanese).
*28 JPCERT Coordination Center, "Improperly setup Asterisk may be exploited for malicious purposes" (http://www.jpcert.or.jp/english/at/2010/at100032.txt).
*29 A technique known as "social spam" was used in these incidents. An explanation of social spam can be found in the following F-Secure blog post. "Social Spam Q&A" (http://www.f-secure.com/weblog/archives/00002079.html).
*30 For example, in the case mentioned in the following Microsoft Malware Protection Center blog post, an attempt to execute malicious files was made by posing as a link to a video. "It's NOT Koobface! New multi-platform infector" (http://blogs.technet.com/b/mmpc/archive/2010/11/03/its-not-koobface-new-multi-platform-infector.aspx).
*31 Details of this incident can be found in the following Arbor Networks' security blog post: "Attack Severs Burma Internet" (http://asert.arbornetworks.com/2010/11/attac-severs-myanmar-internet/).
*32 Details can be found in the following Panda Security blog post. PandaLabs blog, "Tis the Season of DDoS – WikiLeaks Edition" (http://pandalabs.pandasecurity.com/tis-the-season-of-ddos-wikileaks-editio/).
*33 "Akamai Shields Leading Retailers from DDoS Attacks During Critical Holiday Shopping Period" (http://www.akamai.com/html/about/press/releases/2010/press_121310_1.html).

Other

Regarding trends not directly related to incidents, progress was made toward the preparation of infrastructure for the use of DNSSEC in Japan, with DNSSEC signatures for the JP zone beginning in October*34, and a DS record of the JP zone being registered and published to the root zone in December as part of preparations to deploy DNSSEC in the JP zone*35. The IPA also published their "Survey of Denial of Service Attack Countermeasures" report, which summarizes countermeasures for denial of service attacks*36.

1.3 Incident Survey

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

1.3.1 DDoS Attacks

Today, DDoS attacks on corporate servers are almost a daily occurrence. The methods involved in DDoS attacks vary widely. However, most of these attacks are not the type that utilize advanced knowledge such as that of vulnerabilities, but rather cause large volumes of unnecessary traffic to overwhelm network bandwidth or server processes for the purpose of hindering services.

Direct Observations

Figure 2 shows the circumstances of DDoS attacks handled by the IIJ DDoS Defense Service between October 1 and December 31, 2010. 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, and the capacity of the environment attacked (bandwidth and server performance) will largely determine the degree of impact. Figure 2 categorizes DDoS attacks into three types: attacks on bandwidth capacity*37, attacks on servers*38, and compound attacks (several types of attacks on a single target conducted at the same time).

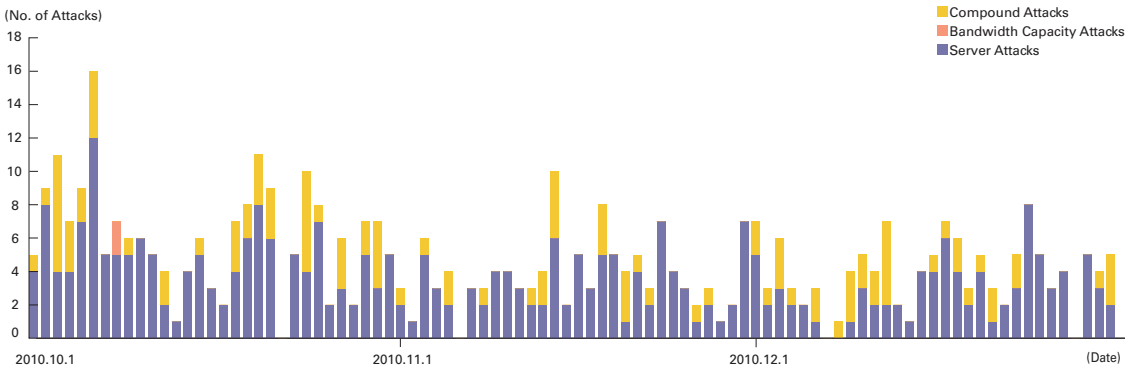


Figure 2: Trends in DDoS Attacks

*34 "Regarding the impact of the start of DNSSEC signatures for the JP zone" (http://jprs.jp/tech/notice/2010-10-15-jp-dnssec.html) (in Japanese).

*35 "Regarding the impact of registering and publishing DS records for the JP zone in the root zone" (http://jprs.jp/info/notice/20101210-ds-published.html) (in Japanese).

*36 IPA (Information Technology Promotion Agency, Japan) "Regarding the 'Survey of Denial of Service Attack Countermeasures' Report" (http://www.ipa.go.jp/security/fy22/reports/isec-dos/index.html) (in Japanese).

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

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

During the three months under study, IIJ dealt with 430 DDoS attacks. This averages to 4.67 attacks per day, indicating a decrease in the average daily number of attacks compared to our prior report. Bandwidth capacity attacks accounted for 0.5% of all incidents, server attacks accounted for 74.7% of all incidents, and compound attacks accounted for the remaining 24.8%.

The largest attack observed during the period under study was classified as a server attack, and resulted in 168Mbps of bandwidth using up to 42,000pps packets. This was also the longest sustained attack, lasting for 15 hours and 20 minutes. Of all attacks, 81.9% ended within 30 minutes of commencement, while 18.1% lasted between 30 minutes and 24 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*39 and botnet*40 usage as the method for conducting DDoS attacks.

■ Backscatter Observations

Next we present our observations of DDoS backscatter using the honeypots*41 set up by the MITF, a malware activity observation project operated by IIJ*42. By monitoring backscatter it is possible to detect DDoS attacks occurring on external networks as a third party without any interposition.

For the backscatter observed between October 1 and December 31, 2010, Figure 3 shows trends in packet numbers by port, and Figure 4 shows the sender's IP addresses classified by country.

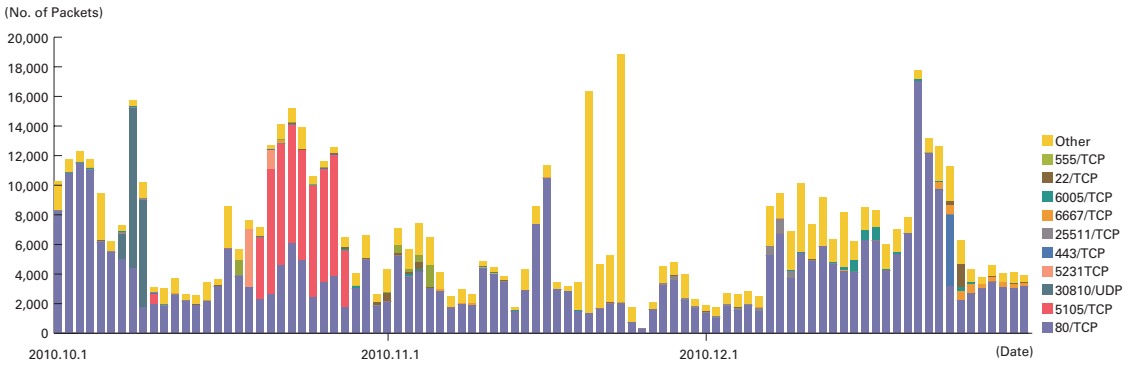


Figure 3: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)

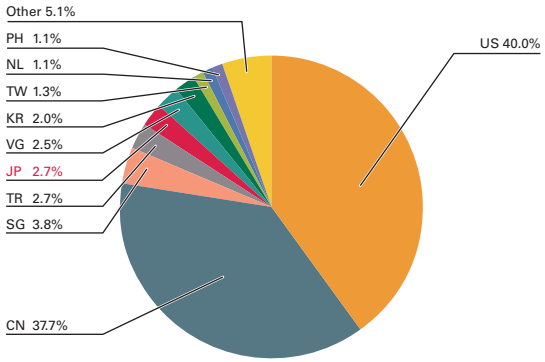


Figure 4: Distribution of DDoS Attack Targets According to Backscatter Observations (by Country, Entire Period under Study)

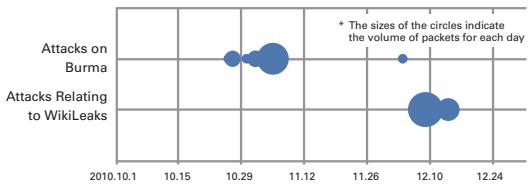


Figure 5: DDoS Attacks on Burma and Relating to WikiLeaks According to Backscatter Observations

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

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

*41 The MITF, a malware activity observation project operated by IIJ, establishes honeypots in order to obtain malware specimens and observe communications arriving over the Internet.

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

The port most commonly targeted by the DDoS attacks observed was the 80/TCP port used for Web services, accounting for 58.9% of the total during this period. Attacks were also observed on other ports used by common services such as 443/TCP, 6667/TCP, and 22/TCP. Looking at the origin of backscatter thought to indicate IP addresses targeted by DDoS attacks by country in Figure 4, the United States and China accounted for large proportions at 40.0% and 37.7%, respectively, and Japan made up 2.7% of the total. During this period backscatter thought to result from attacks on Burma and DDoS attacks relating to WikiLeaks was observed (Figure 5). Backscatter from the attacks on Burma was observed intermittently between October 26 and November 5, 2010. Backscatter relating to WikiLeaks was observed on December 9 with attacks on PayPal and WikiLeaks support site AnonOps.net, and on December 14 with attacks on Amazon.com.

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the MITF*43, a malware activity observation project operated by IIJ. The MITF uses honeypots*44 connected to the Internet in a manner similar to general users in order to observe communications arriving over the Internet. Most appear to be communications by malware selecting a target at random, or scans attempting to locate a target for attack.

■ Status of Random Communications

Figure 6 shows trends in the total volumes of communications coming into the honeypots (incoming packets) between October 1 and December 31, 2010. Figure 7 shows the distribution of sender's IP addresses by country. The MITF has set up numerous honeypots for the purpose of observation. We have taken the average per honeypot, showing the trends for incoming packet types (top ten) over the entire period subject to study.

Much of the communications arriving at the honeypots demonstrated scanning behavior targeting TCP ports utilized by Microsoft operating systems. We also observed scanning behavior for 1433/TCP used by Microsoft's SQL Server and 8080/TCP used for proxies. Additionally, communications of an unknown purpose were observed on ports not used by

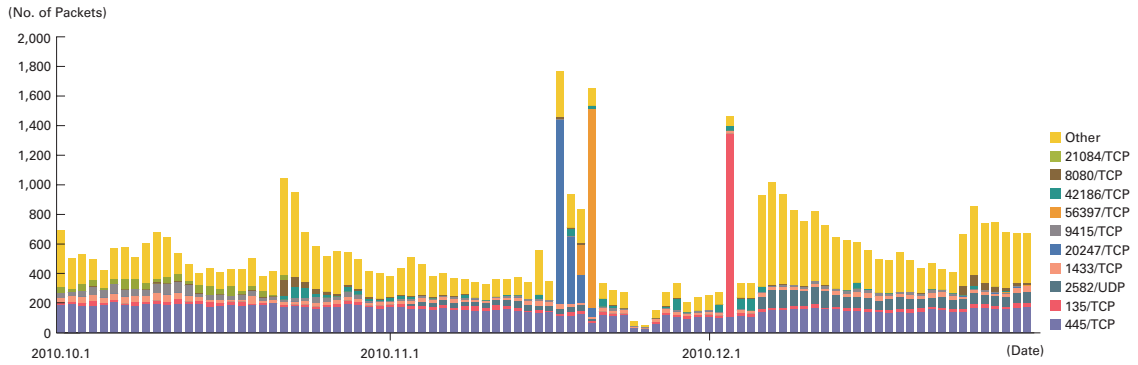


Figure 6: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

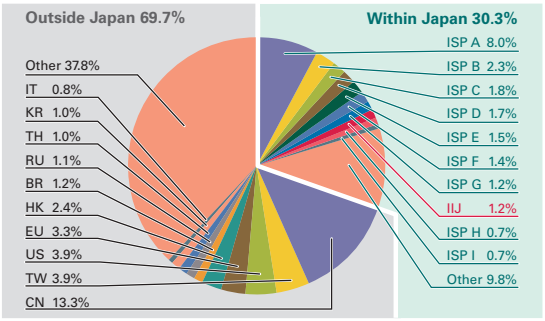


Figure 7: Sender Distribution (by Country, Entire Period under Study)

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

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

common applications, such as 2582/TCP, 20247/TCP, and 9415/TCP. Looking at the overall sender distribution by country in Figure 7, we see that attacks sourced to Japan at 30.3% and China at 13.3% were comparatively higher than the rest.

Malware Network Activity

Figure 8 shows trends in the total number of malware specimens acquired during the period under study. Figure 9 shows the distribution of the specimen acquisition source for malware. In Figure 8, the trends in the number of acquired specimens show the total number of specimens acquired per day*45, while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*46.

On average, 190 specimens were acquired per day during the period under study, representing 30 different malware variants. According to the statistics in our prior report, the average daily total for acquired specimens was 371, with 41 different variants. For this period both the total specimens acquired and the number of different variants declined. This is due to the fact that the activity of Sdbot and its variants ceased completely from late September 2010.

The distribution of specimens according to source country in Figure 9 had Japan at 19.4%, with other countries accounting for the 80.6% balance. Taiwan was at 40.9%, maintaining the large percentage that it held during the previous two report periods. This was due to the heightened activity of Mybot and its variants during this period, which was particularly predominant in Taiwan.

The MITF prepares analytical environments for malware, conducting its own independent analyses of acquired specimens. During the current period under observation 56.8% of the malware specimens acquired were worms, 40.1% were bots, and 3.1% were downloaders. In addition, the MITF confirmed the presence of 25 botnet C&C servers*47 and 29 malware distribution sites. The number of malware distribution sites decreased in comparison to

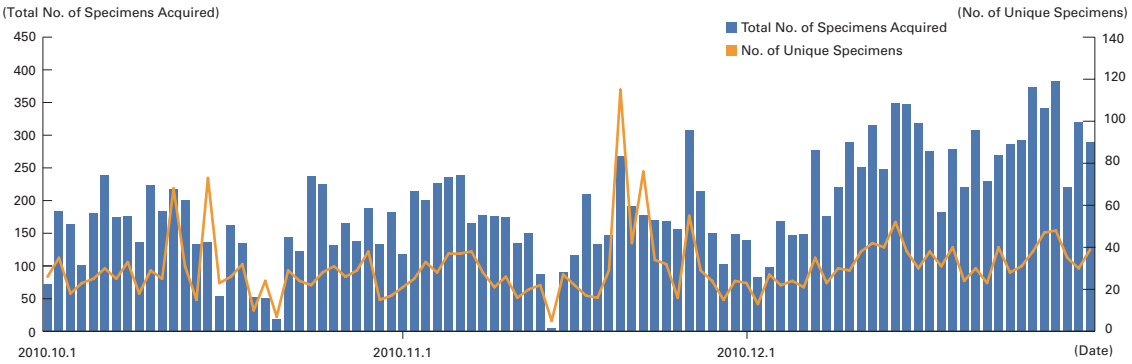


Figure 8: Trends in the Number of Malware Specimens Acquired (Total Number, Number of Unique Specimens)

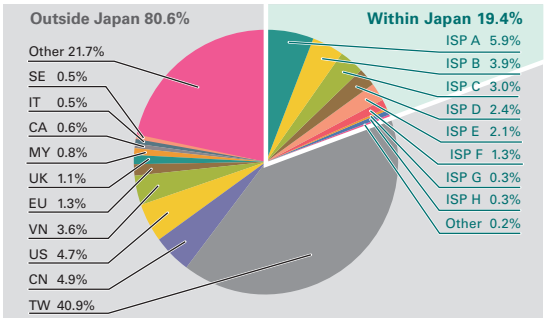


Figure 9: Distribution of Acquired Specimens by Source (by Country, Entire Period under Study)

*45 This indicates the malware acquired by honeypots.

*46 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.

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

the previous report. This can be attributed to the drop in the number of specimens that access multiple distribution sites that were seen in the past.

1.3.3 SQL Injection Attacks

Of the types of different Web server attacks, IIJ conducts ongoing surveys related to SQL injection attacks*48. SQL injection attacks have flared up in frequency numerous times in the past, 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 10 shows trends in the numbers of SQL injection attacks against Web servers detected between October 1 and December 31, 2010. Figure 11 shows the distribution of attacks according to source. These are a summary of attacks detected by signatures on the IIJ Managed IPS Service.

China was the source for 45.4% of attacks observed, while Japan and South Korea accounted for 26.4% and 16.4%, respectively, with other countries following in order. There was very little change from the previous period in the status of SQL injection attacks against Web servers. The overall ratio of attacks from China and Korea increased, and this is because of large-scale attacks on specific addresses sourced mainly to China and Korea that took place between October 6 and 7.

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.

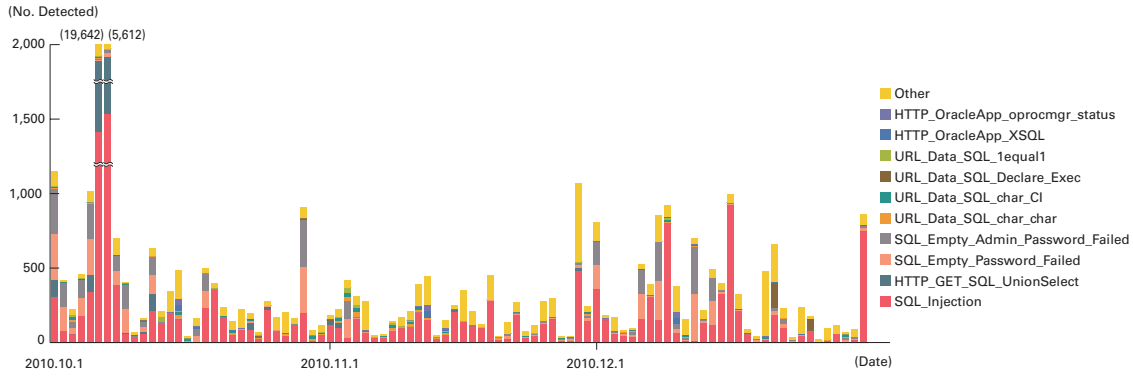


Figure 10: Trends in SQL Injection Attacks (by Day, by Attack Type)

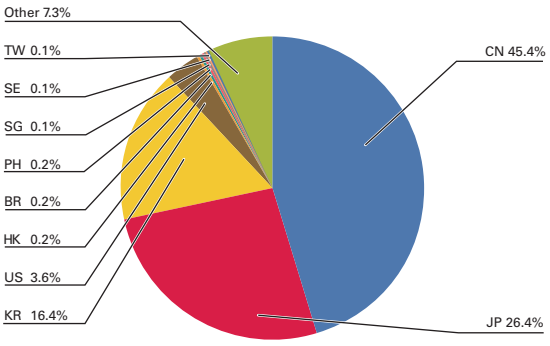


Figure 11: Distribution of SQL Injection Attacks by Source (by Country, Entire Period under Study)

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

1.4 Focused Research

Incidents occurring over the Internet change in type and scope almost from one minute to the next. Accordingly, IIJ works toward taking countermeasures by continuing to perform independent surveys and analyses of prevalent incidents. Here we will present information from the surveys we have undertaken during this period, including an overview of large-scale DDoS attacks that took place in September 2010, malware infections spread through mashup content, and alterations of software distribution packages, as well as the anti-Malware engineering WorkShop 2010 that was held in October.

1.4.1 An Overview of the Large-Scale DDoS Attacks in September 2010

The DDoS attacks that occurred from September to October 2010 had their roots in the collision between Japan Coast Guard patrol vessels and a Chinese vessel off the coast of the Senkaku islands. Advance notice of the targets and time frame of these attacks was given over the Internet, and this incident was also reported by the press. However, the actual form and scale of the attacks has not been disclosed until now. Here we present information gathered by IIJ regarding this series of attacks.

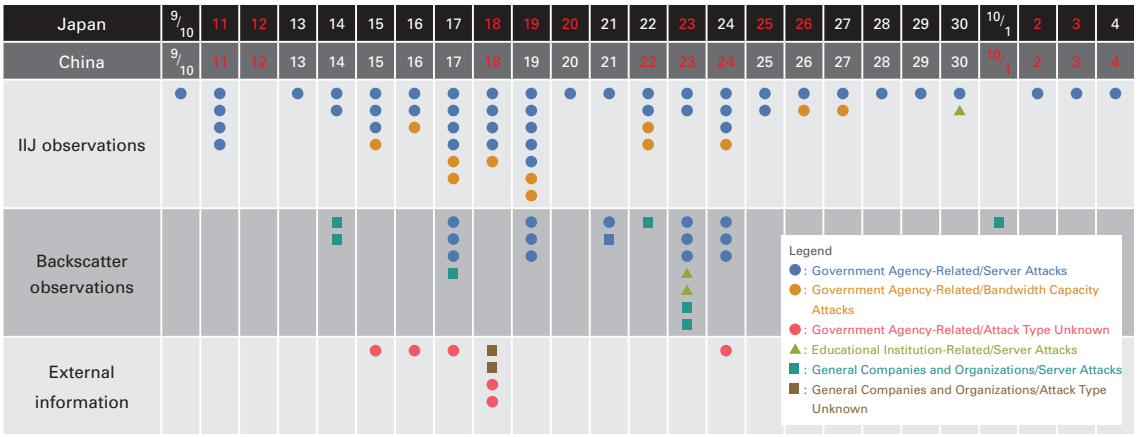
An Overview of the Attacks

An overview of these attacks is shown in Table 1. Since the first attack detected on September 10, attacks of some form or another on a variety of websites were observed each day. Most of the attacks were connection floods that would be categorized as server attacks, but there were also UDP/ICMP flood attacks that fall under the category of bandwidth capacity attacks. The largest server attack observed by IIJ was a connection flood that utilized 5,500,000 simultaneous connections, and the largest bandwidth capacity attack was a UDP/ICMP flood that resulted in over 1.4Gbps of bandwidth. The longest sustained attack on a single website lasted for 291 hours. In addition to direct attack communications from China, there was also communications from countries other than China as well as other domestic ISPs in Japan, and we believe that proxy servers were exploited as stepping stones and that botnets were also utilized. Additionally, there was a small number of SQL injection attacks aimed at altering data, as well as brute force password attacks on FTP servers.

Changing Attack Targets

One characteristic of this series of attacks was the spillover of attacks on to websites not announced in advance. In particular, in the latter half of the attack period attacks were made on sites linked to from websites that were included in the list of attack targets. These linked websites were hosted on servers operated by organizations other than those operating the websites that were the initial targets of the attacks, and it was difficult to understand why they would

Table 1: A Depiction of the Series of Attacks



The marks indicate days in which an attack on specific sites occurred. A single mark is used even when multiple attacks were made on a site on a given day. Combined attacks are classified by the attack type that was identified first. "IIJ observations" indicate attacks on IIJ customers to which IIJ responded. "Backscatter observations" indicate attacks on others in which the IP address was spoofed*49. "External information" indicates information from publicly available sources such as the press etc. The dates in red indicate non-working days (weekends or public holidays) in each country.

*49 See Vol.8 of this report under "1.4.2 Observations on Backscatter Caused by DDoS Attacks" (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol08_EN.pdf) for information regarding the range of data that can be gathered through backscatter observation, as well as its meaning.

be attacked. Some of the smaller websites used servers that were not prepared for DDoS attacks, and it would appear that suitable countermeasures had not been implemented*50.

■ Impact from Attacks

Although attacks began from September 2010, most were handled appropriately by mechanisms such as DDoS defense services, so damage was minimal and the attacks did not become a major topic of discussion. However, by understanding the status of other sites through incidents such as this, one can consider the possibility of attacks spilling over into one's own sites and make provisions. IIJ will continue to provide overviews of attacks such as these, while also deepening ties with other organizations such as ISPs through industry associations and promoting the formulation of mechanisms for gathering data such as this.

1.4.2 Malware Infections Resulting from Mashup Content

Between the end of September and November 2010 servers that provided Web analytics services were intermittently altered, and script that redirected visitors to malicious sites embedded*51. This led to users who viewed sites implementing these services (which included several prominent sites) becoming infected with the malware known as mstmp through drive-by downloads*52, causing widespread damage*53.

■ Incident Characteristics

One of the characteristics of these incidents was the exploitation of pieces of content created through mashups (a method of combining content from multiple sites to present them as a single piece of content). Currently, the APIs for a variety of Web services have been published, and through these it is possible to combine data between sites. Many of the portal sites, search engines, and news sites that the general public view on a daily basis use mashups, with content from multiple sites combined and displayed in a Web browser. This means that if even a single piece of content used in a mashup is altered, malware infections are possible through simply viewing a website using that content (Figure 12).

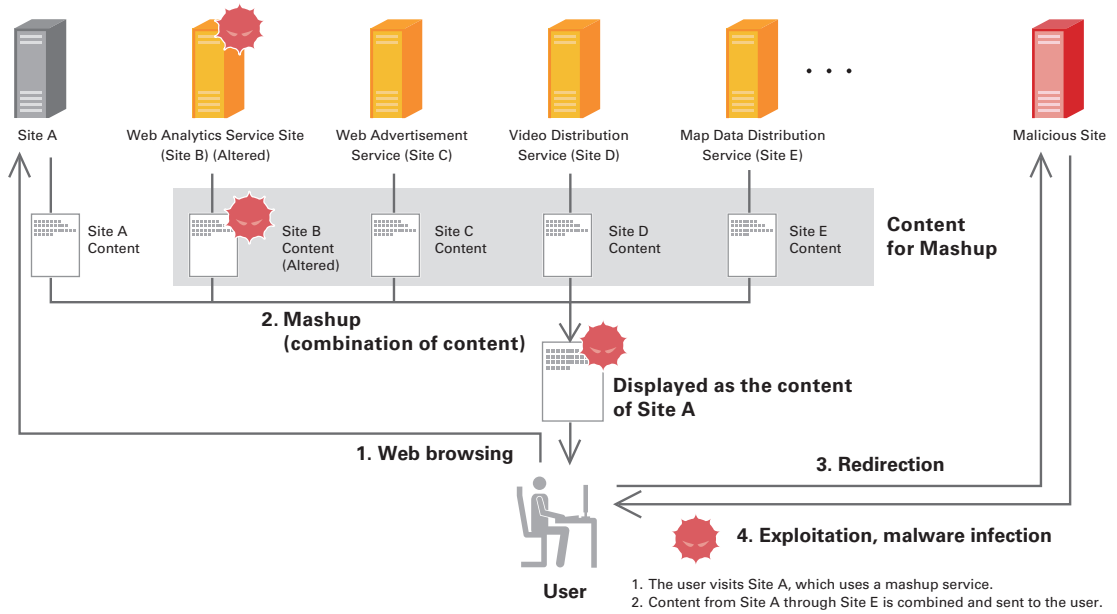


Figure 12: Malware Infections Resulting from Mashup Content

*50 See Vol.9 of this report under "Preparing for DDoS Attacks on Small-Scale Systems" (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol09.pdf) for information regarding protecting small-scale servers from DDoS attacks.

*51 JPCERT Coordination Center, "Web analytics service exploited for malicious purposes" (http://www.jpcert.or.jp/english/at/2010/at100028.txt).

*52 A drive-by download is a method of infecting viewers of Web content with malware undetected by exploiting browser vulnerabilities, etc.

*53 Press reports called this malware "mstmp" from the file name of one of the installed files. The following blog post reports that within Japan at least 100 companies have been infected by this malware. Trend Micro Security Blog: Over 100 Companies Confirmed Infected in Japan. Malicious Program Spreading via Filenames "mstmp" and "lib.dll" (http://blog.trendmicro.co.jp/archives/3723) (in Japanese).

This method is very effective for attackers. In the Gumblar incidents*54 that occurred the year before last, the alteration of websites that provided advertisements to major sites widen the spread of infections. Through the alteration of major advertising sites, there were also multiple cases of users being infected by malware after viewing sites containing these advertisements*55. It has been reported that the number of users infected in the current incident also rose dramatically in a short period of time*56. By simply altering a single piece of commonly-used content, the attacker effectively alters the content of all sites using this content. We can surmise that these kinds of services were targeted intentionally.

The sites using the Web analytics services were innocent sites rather than malicious sites designed for malware distribution. For this reason it was difficult to filter these sites using a blacklist, and we believe this was a contributing factor in the spread of infections.

■ Malware Infections and Subsequent Developments

The malware infections were caused by the redirection of users to malicious sites that attacked vulnerabilities in Web browsers and their plug-ins. IIJ confirmed that the vulnerabilities shown in Table 2 were exploited. Figure 13 shows the behavior of the malware after infection. Once a vulnerability is successfully exploited, a .SWF file with a name consisting of a numeral followed by a decimal point and a 16 digit numeral, such as "1.1234567890123456.swf," is first generated. This file is actually a DLL, and is a program for generating and executing mstmp. The mstmp file operates as a Web browser plug-in to download malware such as lib.dll from an external server, and installs it as a Web browser plug-in. IIJ also noted attacks using a Gumblar-like scheme, with the "Security tool" scareware*57 installed along with malware for stealing FTP accounts, and those accounts being exploited to alter the websites of the infected user.

■ Countermeasures

The best countermeasure is to be aware that malware infections can occur through the viewing of websites and that filtering these sites may be difficult, and swiftly apply patches to browsers and other software*58 on a regular basis. Because it has been reported that attacks targeting vulnerabilities in Java are increasing particularly rapidly*59, it is

Table 2: Vulnerabilities Exploited by mstmp

Software	Version	Vulnerability
MDAC	-	MS06-014
HCP (Help and Support Center)	-	MS10-042
Adobe Reader / Acrobat	< 9.4.0	CVE-2010-3631
Java (JRE)	< 1.6.19	CVE-2010-0094
	< 1.6.19	CVE-2010-0840
	< 1.6.20	CVE-2010-0886

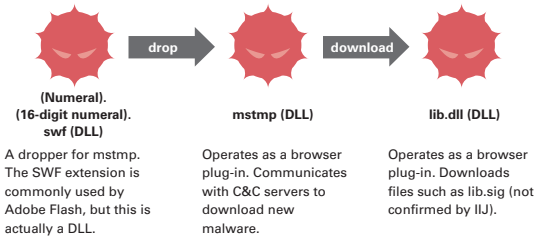


Figure 13: Malware Transitions Following mstmp Infection

*54 Reports on Gumblar and ru:8080 that features a Gumblar-type scheme have been discussed frequently in previous IIR. Vol.4 "1.4.2 ID/Password Stealing Gumblar Malware" (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol04_EN.pdf), Vol.6 "1.4.1 Renewed Gumblar Activity" (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol06_EN.pdf), Vol.7 "ru:8080, Another Attack with a Gumblar-type Scheme" (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol07_EN.pdf).

*55 This incident is also detailed in the following Trend Micro blog post. Adobe zero-day attacks and Web-based threats via ad distribution systems - looking back on threat trends for September 2010 (http://blog.trendmicro.co.jp/archives/3700) (in Japanese).

*56 IBM's Tokyo SOC detected and reported on a sharp increase in malware infections on several occasions. Tokyo SOC Report Regarding the "mstmp" Virus Spread Through Drive-By Download Attacks (https://www-950.ibm.com/blogs/tokyo-soc/entry/dbyd_mstmp_20101027?lang=ja) (in Japanese).

*57 Scareware refers to threats that pose as applications such as security software and issue fake warnings to scare users and defraud them of money. See Vol.3 of this report under "1.4.3 Scareware" (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol03_EN.pdf) for more information about scareware.

*58 It is necessary to stay up-to-date through Windows Update and also maintain the latest versions of browser plug-ins such as Java (JDK, JRE), Adobe Reader/Acrobat, Adobe Flash, and Apple QuickTime.

*59 A surge in exploits targeting Java vulnerabilities has been reported in places such as the following Microsoft Malware Protection Center blog post. Have you checked the Java? (http://blogs.technet.com/b/mmpc/archive/2010/10/18/have-you-checked-the-java.aspx).

crucial to respond quickly to the release of new patches to Java in addition to those for Adobe products that continue to be targeted in recent years. It is also useful to have systems for examining previous firewall and IPS logs after an incident occurs, and systems for finding anomalies by examining and analyzing logs periodically.

1.4.3 Alteration of Software Distribution Packages

Between November 28 and December 2, 2010, a Trojan*60 was distributed together with the ProFTPD*61 source code package*62. This incident occurred because the official server was broken into and files altered. This is not the first time that software distribution packages have been altered in this way. In 1999 TCP Wrappers*63, and in 2002 OpenSSH*64 and Sendmail*65 were altered and packages containing a Trojan distributed in a similar manner. Here we examine the alteration of software distribution packages and methods for detecting such alterations.

■ Alteration of the ProFTPD Distribution Package

The server compromised in this incident served a dual role as both a primary distribution FTP and a synchronization server for mirror servers. Consequently, the altered source code package was distributed to multiple mirror servers that were synchronized over the corresponding period, making it available to a wider number of users. The Trojan that it contained incorporated a back door for acquiring remote shell access in the binary files after they were built, and sent notification to a specific IP address when a user built from the source code.

ProFTPD announced a critical vulnerability on October 29, 2010*66, and released a fixed version on the same day. There were no workarounds via settings for this vulnerability, and with proof of concept code published on November 7, 2010*67, it was extremely dangerous to continue using older versions. The alterations targeted the version containing fixes for this vulnerability, anticipating that many users would update to the new package. However, the altered package differed from the legitimate version, including data such as hash value*68 and digital signature*69 verification results, as well as timestamp and owner data for files in the package that could easily be altered.

■ The Need for Detection of Package Alterations

The majority of widely used open source software is distributed via mirror servers set up on a voluntary basis all over the world. The presence of these mirror servers brings a variety of benefits, such as reducing the load on the primary distribution network and servers, and lowering network latency when users obtain the packages. However, the administrative structure and system composition of each mirror server varies widely, and when a mirror server rather than the primary distribution source is targeted in an attack, there is a chance that packages distributed via that mirror server will be altered. It is also possible that fraudulent packages could be accepted from a distribution source completely unrelated to the original source.

For this reason it is important to check for alterations after a distribution package is obtained, regardless of where it was obtained from. In many cases hash values or signatures are provided by the primary distribution source of the distribution package for detecting alterations. This also applies to the incident in question, as no ill-effects would have been suffered if users who downloaded the package had checked for alterations appropriately.

*60 A type of malware that poses as legitimate software or is combined with a part of it to break into a system. After infiltration it conducts malicious activities when certain conditions (elapsed time or input/output, etc.) are fulfilled. Trojans are often used to steal information, destroy systems, or gain access privileges.
*61 FTP server software. The ProFTPD Project (http://www.proftpd.org/).
*62 This incident was reported on the following ProFTPD site. ftp.proftpd.org compromised (http://forums.proftpd.org/smf/index.php?topic=5206.0).
*63 CA-1999-01: Trojan horse version of TCP Wrappers (http://www.cert.org/advisories/CA-1999-01.html).
*64 CA-2002-24: Trojan Horse OpenSSH Distribution (http://www.cert.org/advisories/CA-2002-24.html).
*65 CA-2002-28: Trojan Horse Sendmail Distribution (http://www.cert.org/advisories/CA-2002-28.html).
*66 CVE-2010-4221: Telnet IAC processing stack overflow (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4221).
*67 Full Disclosure: ProFTPD IAC Remote Root Exploit (http://seclists.org/fulldisclosure/2010/Nov/49).
*68 MD5 (Message Digest 5) and SHA-1 (Secure Hash Algorithm 1) are examples of widely used hash algorithms.
*69 GnuPG (http://www.gnupg.org/) is an example of software compatible with digital signatures using public key cryptography.

■ Alteration Detection using Hash Values

Figure 14 shows an example of alteration detection using hash values. Alterations can be detected by comparing the hash value with the downloaded package. However, as hash values can be easily generated, if the package is altered there is a chance that the hash value accompanying it has also been altered. Consequently, when performing alteration detection using hash values, it is necessary to obtain a hash value from a source other than the one from which the package was obtained, such as the Web server operated by the primary distribution source.

Many distribution packages provide hash values derived from the MD5 algorithm. However, the MD5 algorithm has already been compromised, so it is dangerous to use it for detecting alterations. On November 30, 2007 a demo showing the creation of files with different content that had the same hash value was released, proving that the compromise of the MD5 algorithm was no longer merely theoretical*70. As a result, although careless alterations such as those for the current incident can be detected, the detection of alterations using hash values as the primary method is not sufficient.

■ Alteration Detection using Digital Signatures

Figure 15 shows an example of alteration detection using digital signatures. Digital signatures require a private key for generation and a public key for verification, making it extremely difficult to maintain integrity while carrying out alterations. Consequently, it is possible to detect alterations using the digital signatures distributed along with packages. However, it is necessary to note that those perpetrating alterations are able to generate a separate key themselves and use that to sign an altered package in order to generate a digital signature that maintains integrity. In this case, it is presumed that the public key of the altering party is also distributed along with the package.

When using an unknown public key, it is necessary to acquire a fingerprint*71 of the key from a source other than the one the key was obtained from, and cross-check this to verify that it is a valid key that can be trusted. As the legitimacy of a public key must first be investigated, it is slightly more complex than detection using hash values. However, the reliability of detection using digital signatures is based on a set of legitimate private and public keys. Because there is no point in using a public key generated by the one who altered a package, it is best to obtain a valid public key that can be trusted in advance, rather than blindly trusting an unknown public key.

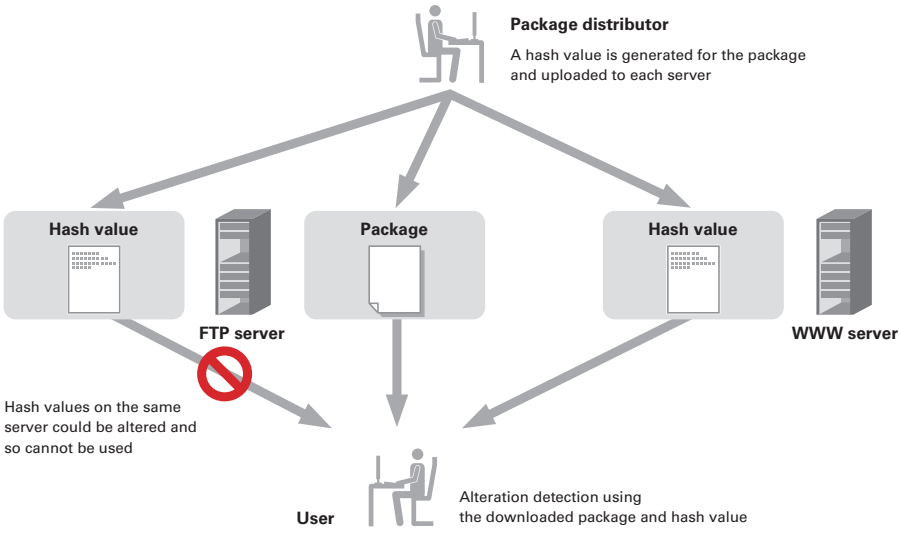


Figure 14: An Example of Detecting Alterations using Hash Values

*70 Predicting the winner of the 2008 US Presidential Elections using a Sony PlayStation 3 (http://www.win.tue.nl/hashclash/Nostradamus/). See Vol.8 of this report under "1.4.1 Trends in the Year 2010 Issues on Cryptographic Algorithms" (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol08_EN.pdf) for more information on the compromise of cryptographic algorithms.

*71 The hash value of a public key used in a public key encryption method.

■ Automatic Verification of Distribution Packages

Similar measures are adopted for the distribution of binary files. Digital signatures are embedded in the RPM (Redhat Package Manager) format packages used in Red Hat's Linux distribution RHEL (Red Hat Enterprise Linux) as well as in Microsoft's Windows, making automatic verification possible and allowing users to identify the distributor.

■ Summary

Here, we gave an overview of the ProFTPD distribution package alteration incident, and explained methods for detecting altered packages. There is no point in updating to fix a vulnerability only to end up installing a Trojan horse. Once a system is compromised, it is very hard to ensure security even when the root cause is eliminated. For this reason, it is important to make the effort to detect for alterations when implementing packages.

1.4.4 The anti-Malware engineering WorkShop 2010

The anti-Malware engineering WorkShop 2010 (MWS2010)*72 was held over three days from October 19 to October 21, 2010. The workshop, which is hosted by the Cyber Clean Center*73 Steering Committee and the Information Processing Society of Japan, began in 2008 as a place for sharing the results of malware countermeasure research using a common research data set*74.

The data set used for research was CCC DATAset 2010, which is based on Cyber Clean Center observation data for malware that spreads via networks. This time both the number of data items and the target period were more comprehensive than the previous year. Malware specimen activity data and Web malware data sets provided by the researcher community were added, resulting in an increased number of variants for analysis.

■ Research Presented

22 verbal presentations were given at MWS2010*75. Several presentations detailed attempts to define regular hosts and malicious hosts through statistical processing of IP addresses and URLs as well as associated attribute

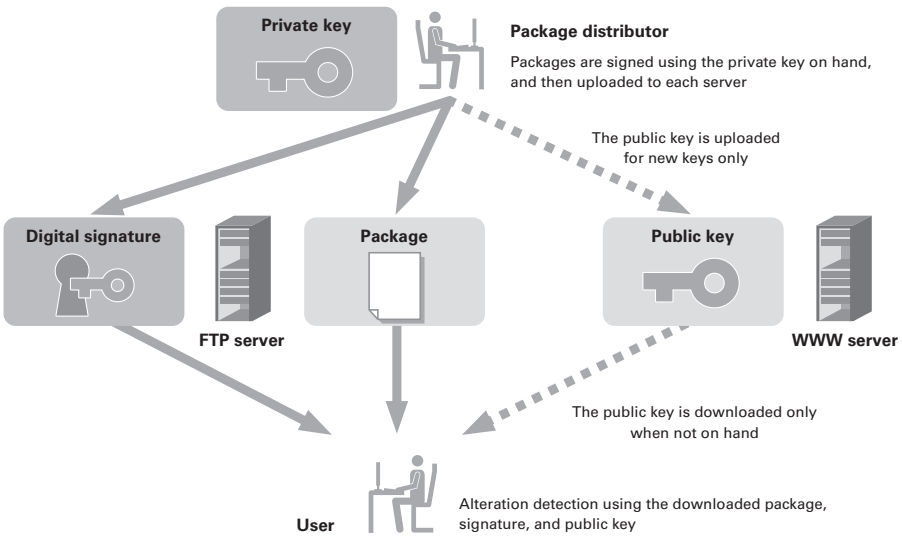


Figure 15: An Example of Detecting Alterations using Digital Signatures

*72 anti-Malware engineering WorkShop 2010 (http://www.iwsec.org/mws/2010/en.html). Held concurrently with the Computer Security Symposium 2010, organized by the Computer Security Group of the Information Processing Society of Japan (http://www.iwsec.org/css/2010/english/index.html).

*73 The Cyber Clean Center is a bot countermeasure project initiated by the Ministry of Internal Affairs and Communications, the Ministry of Economy, Trade and Industry, as well as other related organizations (https://www.ccc.go.jp/en_ccc/index.html).

*74 See Vol.5 of this report under "Internet Topics: About the anti-Malware engineering WorkShop 2009" (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol05_EN.pdf) for information regarding last year's workshop.

*75 See the papers and presentation materials published at the following URL for more information. MWS 2010 in pictures (http://www.iwsec.org/mws/2010/photo.html) (in Japanese).

information (DNS and whois information, etc.). Research into the effective analysis of malware was also presented from a variety of perspectives, including countermeasures involving the development and improvement of VMM (Virtual Machine Monitor) and emulators. Other presentations covered a broad range of research such as methods for visualizing attack-related data, methods for detecting unknown malware, attack and malware classification methods, and the results of analyzing malware activity based on network distance, leading to many vibrant discussions.

IIJ followed up on its work from MWS2008 and MWS2009 by presenting the results of comparing observation data from the MITF honeypot network and CCC DATAset 2010 attack source data from the research data set, highlighting differences between them and changes over time. We also presented the conclusions we drew from simulations of the relationship between filter scope and time lag leading up to the application of filters and the success rate of defensive measures, assuming countermeasures in which attack source addresses discovered on an observation network are filtered on a network.

■ MWS Cup 2010

As with last year, the MWS Cup 2010 was held to compete over technology for analyzing a given set of communications data within a specified time. Eight teams including six student teams competed in the event, with each bringing their own analysis environment and vying over technology and accuracy. IIJ also took part, applying a newly developed analysis tool. While we were unable to beat one of the student teams and take home overall 1st place, we were awarded 2nd place and winner of the technical category. At the anti-Malware engineering WorkShop, data sets reflecting recent malware trends and research findings based on these data sets were shared. IIJ considers this a valuable opportunity for exchanging opinions regarding current Internet threats and their countermeasures with members of the scientific community that we rarely have the chance to interact with during the regular course of business, and we plan to continue to actively participate in this event in the future.

1.5 Conclusion

This report has provided a summary of security incidents to which IIJ has responded. In this report we discussed the DDoS attacks that took place in September 2010, malware infections resulting from mashup content, and alterations of software distribution packages. We also provided an overview of MWS2010, where research on malware analysis is presented.

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

Authors:
Mamoru Saito
Manager of the Office of Emergency Response and Clearinghouse for Security Information, IIJ Service Division. After working in security services development for enterprise customers, Mr. Saito became the representative of the IIJ Group emergency response team, IIJ-SECT in 2001, participating in FIRST, an international group of CSIRTs. Mr. Saito serves as a steering committee member of several industry groups, including Telecom-ISAC Japan, Nippon CSIRT Association, Information Security Operation provider Group Japan, the Web Malware Mitigate Community, and others. He is also active in multiple organizations such as the Council for Stable Operation of the Internet, the Engineers SWG of the Working Committee for Child Pornography Countermeasures in the Association for Promoting the Creation of a Safe Internet, and the IPA Conference for Denial of Service Attack Countermeasures.

Hirohide Tsuchiya (1.2 Incident Summary)
Hirohide Tsuchiya, Hiroshi Suzuki, Tadaaki Nagao (1.3 Incident Survey)
Mamoru Saito, Hiroaki Yoshikawa (1.4.1 Large-Scale DDoS Attacks in September 2010)
Hiroshi Suzuki (1.4.2 Malware Infections Resulting from Mashup Content)
Tadashi Kobayashi (1.4.3 Alteration of Software Distribution Packages)
Tadaaki Nagao (1.4.4 The anti-Malware engineering WorkShop 2010)
Office of Emergency Response and Clearinghouse for Security Information, IIJ Service Division

Contributors:
Masahiko Kato, Yuji Suga, Takahiro Haruyama, Seigo Saito, Office of Emergency Response and Clearinghouse for Security Information, IIJ Service Division