Targeted Attacks and Operation Aurora

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

1.1 Introduction

This report summarizes incidents to which IIJ responded, based on general information obtained by IIJ itself related to the stable operation of the Internet, information from observations of incidents, information acquired through our services, and information obtained from companies and organizations with which IIJ has cooperative relationships. This volume covers the period of time from January 1 through March 31, 2010. In this period incidents of Gumblar and similar malware designed to steal IDs and passwords that we examined in our last report continued to occur, and many website alterations related to these incidents have been reported. A series of vulnerabilities that affect Web browsers and servers were also discovered. Besides these there was also a hijacking incident in which DNS information was manipulated without authorization, and SEO poisoning incidents that took advantage of a natural disaster. Targeted attacks on a number of major U.S. corporations were also a major topic. As seen above, the Internet continues to experience many security-related incidents.

1.2 Incident Summary

Here, we discuss the IIJ handling and response to incidents that occurred between January 1 and March 31, 2010. Figure 1 shows the distribution of incidents handled during this period*1.

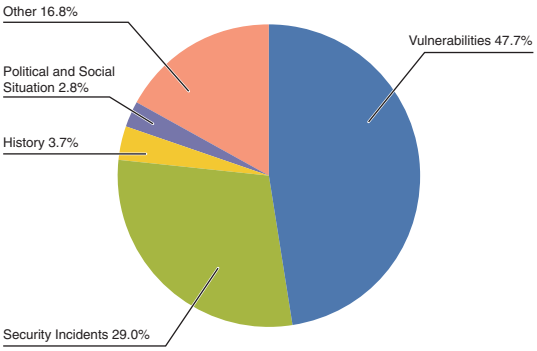


Figure 1: Incident Ratio by Category (January 1 to March 31, 2010)

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

■ Vulnerabilities

During this period a large number of vulnerabilities related to Web browsers and their plug-ins were discovered and fixed, including Microsoft's Internet Explorer*2*3, Adobe Systems' Adobe Reader, Adobe Acrobat*4*5, Adobe Flash Player*6*7, and the Adobe Download Manager*8 that is used for product updates, RealNetworks' RealPlayer*9, and Oracle's Java Runtime Environment (JRE)*10. Several of these vulnerabilities were exploited before patches were released.

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

■ Political and Social Situations

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

■ History

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

■ Security Incidents

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

■ Other

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

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

1.3 Incident Survey

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

1.3.1 DDoS Attacks

Today, DDoS attacks on corporate servers are almost a daily occurrence. The methods involved in DDoS attacks vary widely. Generally, however, these attacks are not the type that utilize advanced knowledge such as that of vulnerabilities, but rather cause large volumes of unnecessary traffic to overwhelm network bandwidth or server processes for the purpose of hindering services. Figure 2 shows the circumstances of DDoS attacks handled by the IIJ DDoS Defense Service between January 1 and March 31, 2010.

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

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

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

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

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

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

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

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

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

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

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

During the three months under study, IIJ dealt with 227 DDoS attacks. This averages to 2.52 attacks per day, indicating that there was no significant change in the average daily number of attacks compared to our prior report.

Bandwidth capacity attacks accounted for 0% of all incidents. Server attacks accounted for 86% of all incidents, and compound attacks accounted for the remaining 14%. The largest attack observed during the period under study was classified as a server attack, and resulted in 105Mbps of bandwidth using 30,000pps packets. Of all attacks, 86% ended within 30 minutes of commencement, while 14% lasted between 30 minutes and 24 hours. During the time period under study, IIJ did not note any attacks that exceeded 24 hours in length.

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

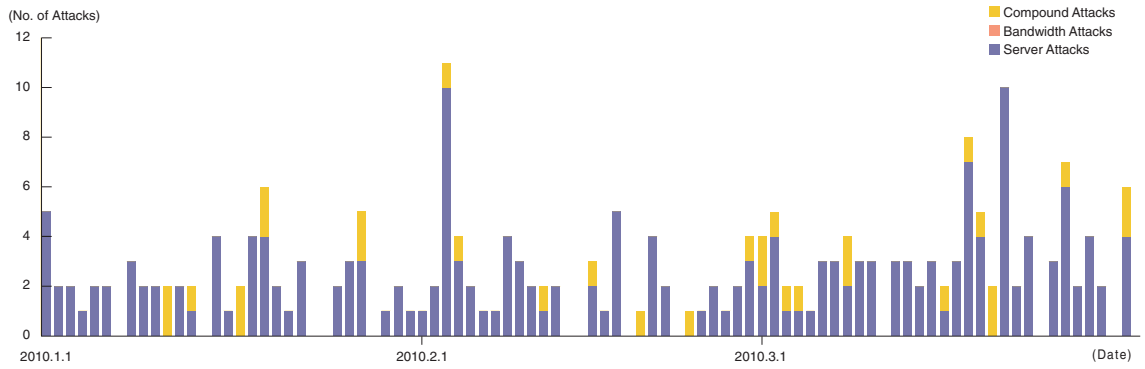


Figure 2: Trends in DDoS Attacks

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

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

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

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

1.3.2 Malware Activities

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

■ Status of Random Communications

Figure 3 shows trends in the total volumes of communications coming into the honeypots (incoming packets) between January 1 and March 31, 2010. Figure 4 shows the distribution of sender's IP addresses by country. The MITF has set up numerous honeypots for the purpose of observation. We have taken the average per honeypot, showing the trends for incoming packet types (top ten) over the entire period subject to study.

Much of the communications arriving at the honeypots demonstrated scanning behavior targeting TCP ports utilized by Microsoft operating systems. As with the prior study, we observed scanning behavior for 2967/TCP used by Symantec client software and 22/TCP used for SSH. At the same time, communications for which the goal was not clearly identifiable, such as 2582/TCP and 11999/TCP (not used by general applications), were also observed. Looking at the overall sender distribution by country, we see that attacks sourced to China at 17.9%, Japan at 15.9%, and Vietnam at 9.9% were comparatively higher than the rest.

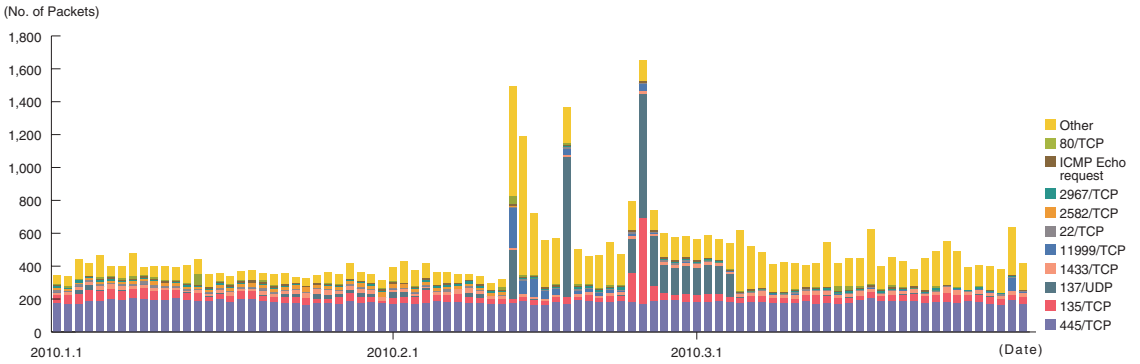


Figure 3: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

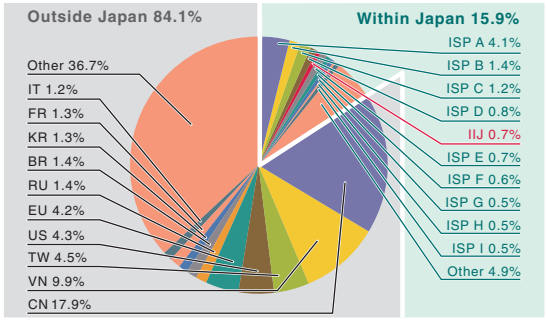


Figure 4: Sender Distribution (by Country, Entire Period under Study)

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

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

Malware Network Activity

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

On average, 479 specimens were acquired per day during the period under study, representing 37 different malware variants. According to the statistics in our prior report, the average daily total for acquired specimens was 623, with 44 different variants. For this period both the total specimens acquired and the number of different variants declined compared to the previous period.

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

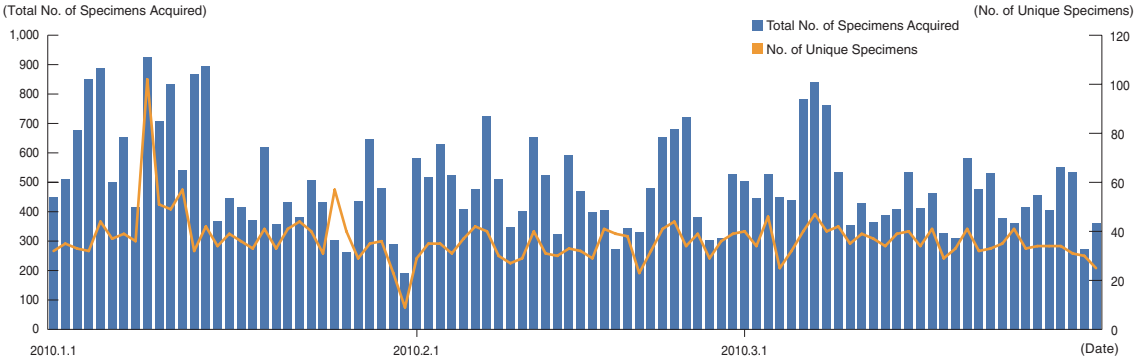


Figure 5: Trends in the Number of Malware Specimens Acquired (Total Number, Number of Unique Specimens)

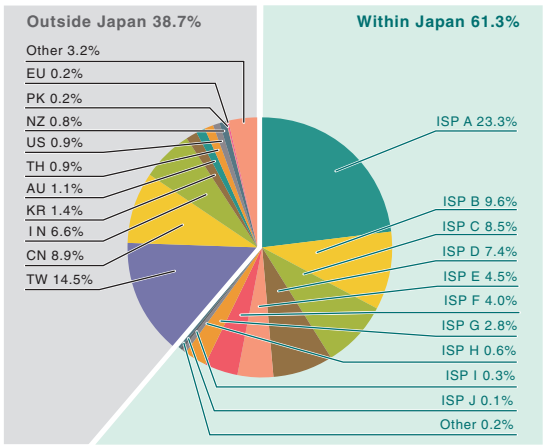


Figure 6: Distribution of Acquired Specimens by Source (by Country, Entire Period under Study)

*37 This indicates the malware acquired by honeypots.

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

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

1.3.3 SQL Injection Attacks

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

Figure 7 shows trends of the numbers of SQL injection attacks against Web servers detected between January 1 and March 31, 2010. Figure 8 shows the distribution of attacks according to source. These are a summary of attacks detected by signatures on the IIJ Managed IPS Service. Japan was the source for 60.4% of attacks observed, while China and the United States accounted for 10.0% and 9.5%, respectively, with other countries following in order. We noted the number of SQL injection attacks on Web servers similar to our prior report.

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

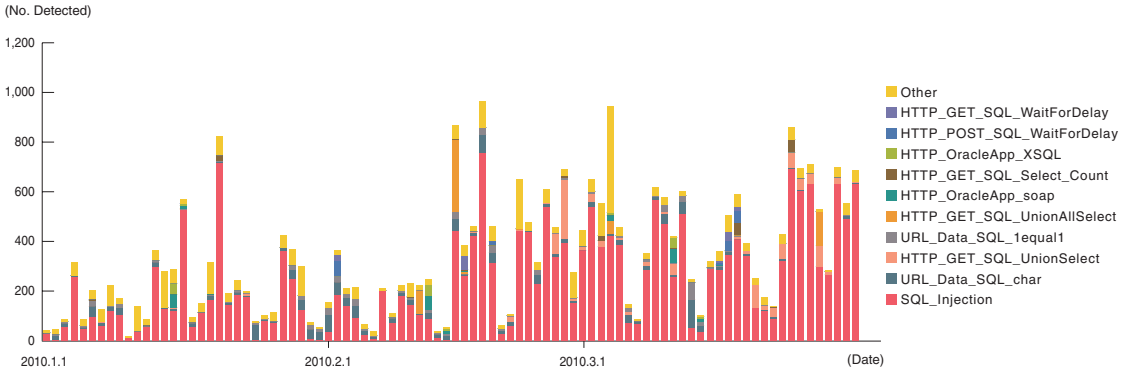


Figure 7: Trends in SQL Injection Attacks (by Day, by Attack Type)

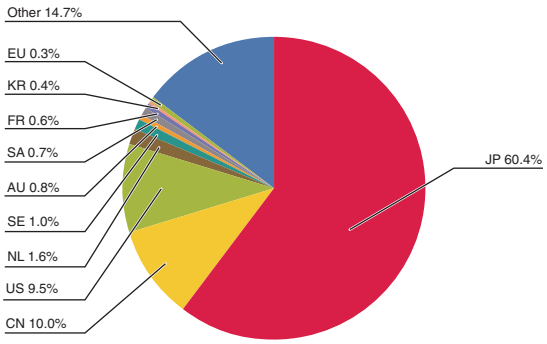


Figure 8: Distribution of SQL Injection Attacks by Source (by Country, Entire Period under Study)

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

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

1.4 Focused Research

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

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

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

■ Differences to Gumblar

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

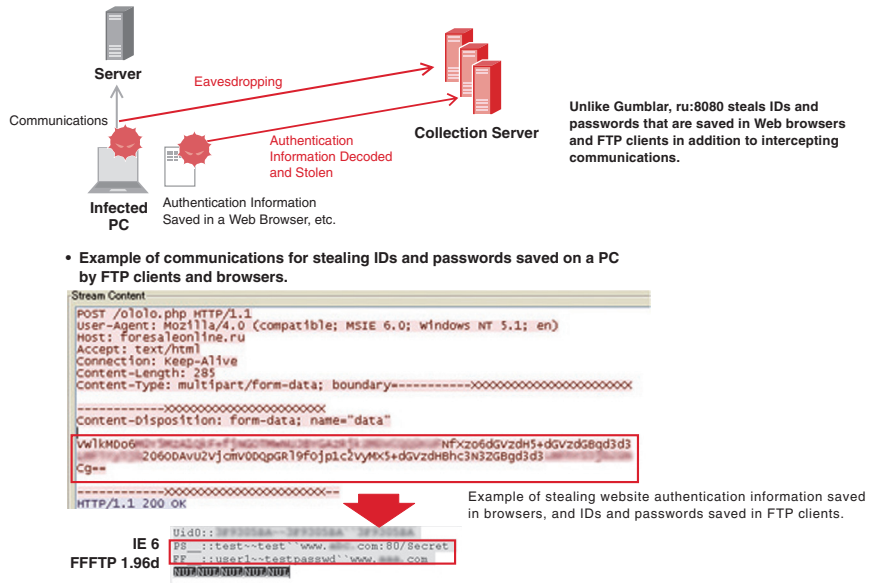


Figure 9: How ru:8080 Steals IDs and Passwords

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

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

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

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

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

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

Malware Behavior

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

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

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

Table 1: Comparison of Vulnerabilities Exploited

Work Towards a Countermeasure

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

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

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

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

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

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

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

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

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

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

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

1.4.2 Targeted Attacks and Operation Aurora

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

■ Targeted Attacks on Specific Entities

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

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

■ Examples of Targeted Attacks

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

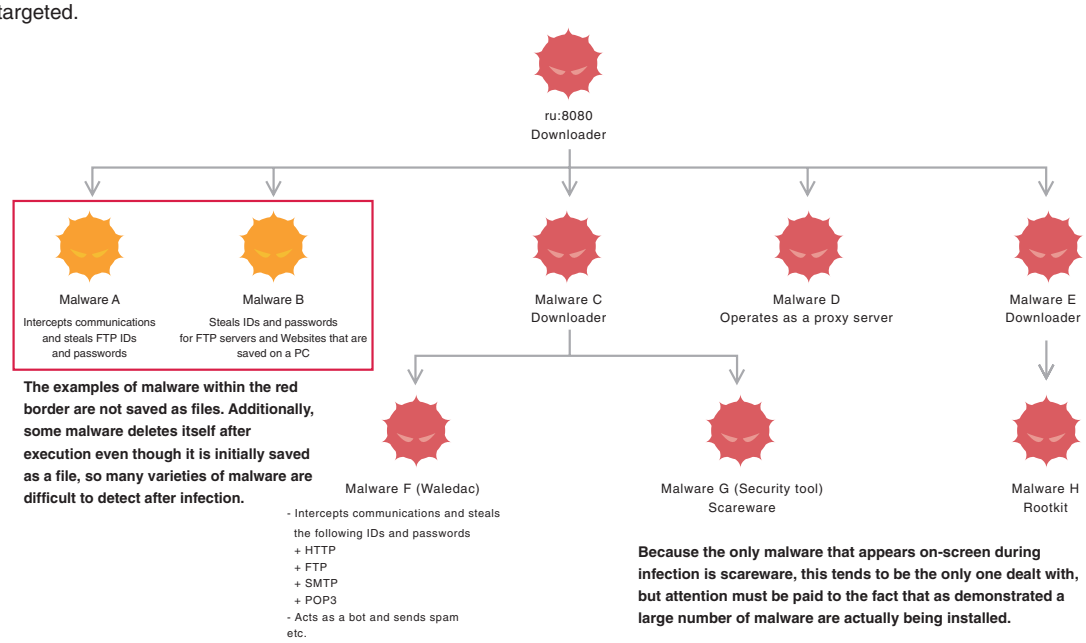


Figure 10: List of Malware Installed by ru:8080

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

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

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

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

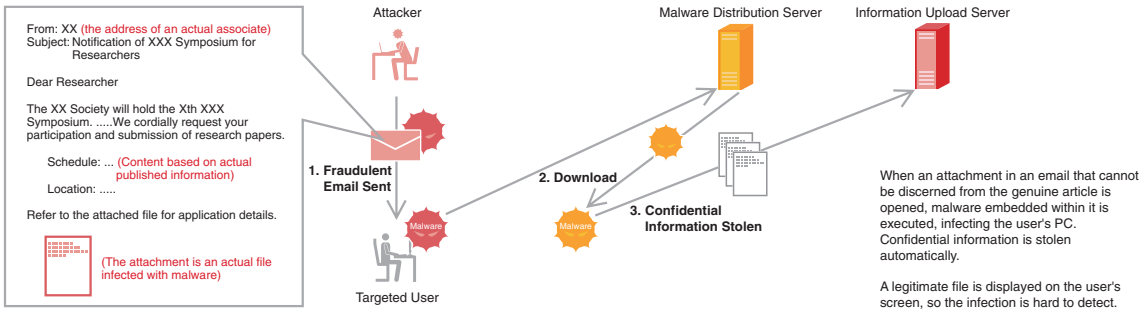
In June of 2008, a targeted attack that posed as an announcement soliciting papers for a computer security symposium took place*57. The body of the email was cut and pasted from a legitimate message, and sent along with an attachment that was created by embedding malware into a legitimate PDF file. The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

■ Operation Aurora

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

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

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



▶ **Operation Aurora Attacks**

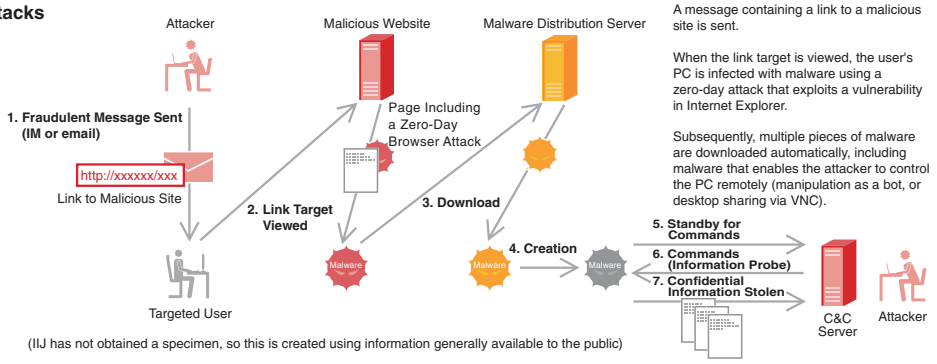


Figure 11: Targeted Attacks Using Fraudulent Email

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

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

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

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

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

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

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

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

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

■ The Difficulty of Dealing with Targeted Attacks

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

1.4.3 MITF Anti-Malware Activities

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

■ Methods for Obtaining Malware

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

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

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

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

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

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

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

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

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

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

■ Methods for Analyzing Malware

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

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

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

■ MITF Overview and Future Plans

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

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

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

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

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

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

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

1.5 Conclusion

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

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

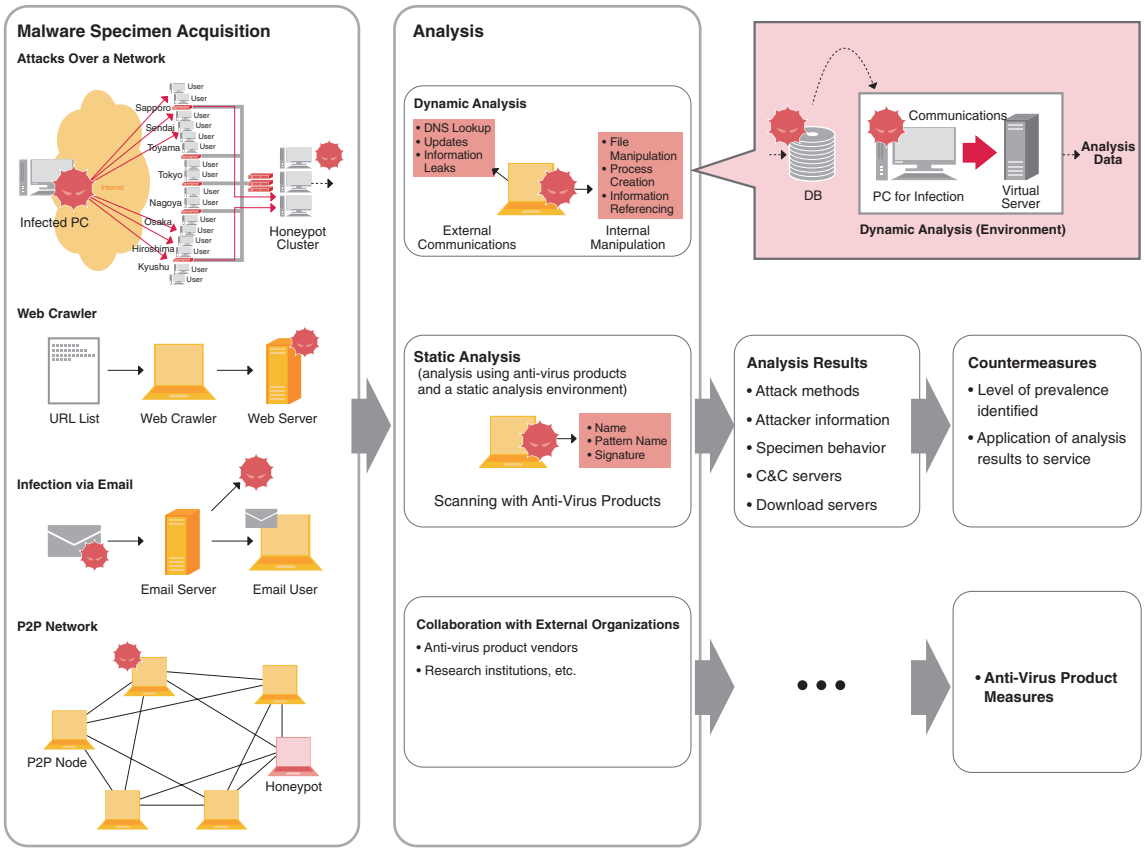


Figure 12: MITF Framework

Authors:

Mamoru Saito

Manager of the Office of Emergency Response and Clearinghouse for Security Information, IIJ Service Division. After working in security services development for enterprise customers, Mr. Saito became the representative of the IIJ Group emergency response team, IIJ-SECT in 2001, participating in FIRST, an international group of CSIRTs. Mr. Saito serves as a steering committee member of several industry groups, including Telecom-ISAC Japan, Nippon CSIRT Association, Information Security Operation provider Group Japan, the Web Malware Mitigate Community, and others. In recognition of its close activities with both domestic and international organizations, the IIJ-SECT was awarded the "commendation from Director-General, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry (CATEGORY - Promotion of Information Security)" at the FY 2009 Informatization Month Opening Ceremony.

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

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