The 3.20 Cyber Attack in South Korea

In this report, we will discuss a large-scale incident that occurred in South Korea in March, in addition to incidents of malware infection in Japan caused by rogue Apache modules. We will also take a look at exercises for responding to cyber attacks.

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, 2013. In this period a number of hacktivism-based attacks were made by Anonymous and other groups, following on from those in the last survey period. A series of targeted attacks on companies and government-related institutions were also identified, and the details of several attacks were published in reports. In March, major attacks involving malware occurred in South Korea, and a large-scale DDoS attack said to have reached 300 Gbps was made in Europe. In Japan, messages from the culprit behind the "Remote Control Virus" were released a number of times, and a suspect was arrested in February. 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, 2013. Figure 1 shows the distribution of incidents handled during this period*1.

■ The Activities of Anonymous and Other Hacktivists

Attacks by hacktivists such as Anonymous continued during this period. DDoS attacks and information leaks occurred at government-related and company sites in a large number of countries stemming from a variety of incidents and causes. Notable incidents included attacks on sites related to the Israeli government (#OpIsrael), and attacks from the Israeli side targeting Palestine believed to have been made as reprisal for these. Attacks also continued to be made on government institutions in Egypt (#OpEgypt) and other countries.

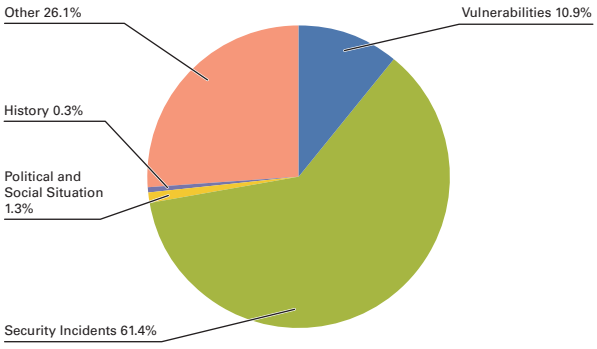


Figure 1: Incident Ratio by Category (January 1 to March 31, 2013)

In January, DDoS attacks and website alterations targeted the Massachusetts Institute of Technology (MIT) in relation to the suicide of an Internet activist who had been accused of breaking into the MIT facility and stealing academic articles. A number of other websites were also altered in connection with this, including the website of the United States Sentencing Commission. Anonymous continued to

*1 Incidents discussed in this report are categorized as vulnerabilities, political and social situations, history, security incidents or 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.

be very active, releasing encrypted files thought to have been obtained through these activities, as well as the personal information of individuals associated with U.S. banks (#OpLastResort).

TeamGhostShell broke into the servers of a number of universities, government institutions, and private-sector businesses in Africa, and released 700,000 pieces of account information (#ProjectSunRise). A third round of DDoS attacks on U.S. banks began in March (Operation Ababil), the latest in a series that have occurred on and off since last year. These examples demonstrate that groups other than Anonymous also continue to be active.

■ Vulnerabilities and their Handling

During this period fixes were released for Microsoft's Windows*2*3*4*5*6 and Internet Explorer*7*8*9. Updates were also made to Adobe Systems' Flash Player, Reader, and Acrobat. A number of updates including unscheduled ones were made to Oracle's Java, fixing many vulnerabilities. A vulnerability that allowed malicious programs to be executed was discovered and fixed in JustSystems Corporation's Ichitaro and Hanako software products, which are often used at public agencies in Japan. Several of these vulnerabilities were exploited before patches were released.

Regarding server applications, a quarterly update for the Oracle database server was released, fixing many vulnerabilities. A vulnerability in BIND9 DNS servers that caused abnormal server termination through the use of large amounts of memory was also fixed.

A number of vulnerabilities that could allow circumvention of authentication by third parties, execution of arbitrary code, and execution of arbitrary SQL commands through parameter parsing were discovered and fixed in the highly popular Web application framework Ruby on Rails.

Multiple vulnerabilities that could allow a buffer overflow through SSDP request processing were also discovered and fixed in the UPnP (Universal Plug and Play) library used with many network devices. Because UPnP is used in many devices such as household broadband routers, Web cameras, and IP telephony equipment, U.S. security firm Rapid7 published a white paper summarizing UPnP-related security issues and matters of concern*10. The JPCERT Coordination Center also issued a warning, because many vendors did not implement a fix, and even when there was one many users did not apply it*11.

■ DDoS Attacks Using Open DNS Resolvers

In March, the Spamhaus anti-spam organization was targeted by a massive DDoS attack. This attack was initially directed at Spamhaus's website, as well as the equipment of CloudFlare, which intervened to counter it. It ultimately lasted for six days while switching targets several times, including targeting the equipment of the Internet exchange that CloudFlare connects to.

It is thought that DNS amplification was used in this attack. DNS amplification attacks direct large volumes of data at the target by spoofing their IP address and issuing DNS queries, which can generate large responses. This is thought to have the effect of concealing the identity of the attacker, while also making it appear to the target as if they are being attacked from around the world using DNS resolvers accessible from the Internet as stepping stones. For this reason US-CERT issued

*2 "Microsoft Security Bulletin MS13-002 - Critical: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (2756145)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-002).

*3 "Microsoft Security Bulletin MS13-010 - Critical: Vulnerability in Vector Markup Language Could Allow Remote Code Execution (2797052)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-010).

*4 "Microsoft Security Bulletin MS13-020 - Critical: Vulnerability in OLE Automation Could Allow Remote Code Execution (2802968)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-020).

*5 "Microsoft Security Bulletin MS13-022 - Critical: Vulnerability in Silverlight Could Allow Remote Code Execution (2814124)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-022).

*6 "Microsoft Security Bulletin MS13-027 - Important: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege (2807986)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-027).

*7 "Microsoft Security Bulletin MS13-008 - Critical: Security Update for Internet Explorer (2799329)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-008). (Unscheduled)

*8 "Microsoft Security Bulletin MS13-009 - Critical: Cumulative Security Update for Internet Explorer (2792100)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-009).

*9 "Microsoft Security Bulletin MS13-021 - Critical: Cumulative Security Update for Internet Explorer (2809289)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-021).

*10 US-CERT, "Vulnerability Note VU#922681 Portable SDK for UPnP Devices (libupnp) contains multiple buffer overflows in SSDP" (http://www.kb.cert.org/vuls/id/922681).

*11 JPCERT/CC, "JPCERT/CC Alert 2013-01-31 Vulnerability in Portable SDK for UPnP" (http://www.jpcert.or.jp/english/at/2013/at130006.html).

January Incidents

1 **S** **1st:** It was reported that a number of pieces of confidential information may have been leaked due to incidents of virus infection at the Ministry of Agriculture, Forestry and Fisheries last year.

2 **S** **1st:** Email messages from the individual thought to be responsible for the "Remote Control Virus" incident were sent to a number of news outlets and reporters.

3 **S** **4th:** After the discovery in December of fraudulent digital certificates originating from the issue of fraudulent intermediate certificates by Turkish certificate authority TURKTRUST, involved companies announced these certificates had been revoked.
See the following Google Online Security Blog post for more details. "Enhancing digital certificate security" (http://googleonlinesecurity.blogspot.jp/2013/01/enhancing-digital-certificate-security.html).

4

5 **S** **5th:** Email messages from the individual thought to be responsible for the "Remote Control Virus" incident were once again sent to a number of news outlets and reporters.

6 **V** **9th:** A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB13-01: Security updates available for Adobe Flash Player" (http://www.adobe.com/support/security/bulletins/apsb13-01.html).

7

8 **V** **9th:** A number of vulnerabilities in Adobe Reader and Acrobat that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB13-02: Security updates for Adobe Reader and Acrobat" (http://www.adobe.com/support/security/bulletins/apsb13-02.html).

9 **V** **9th:** A number of vulnerabilities (CVE-2013-0156) in the parameter parsing for Ruby on Rails Action Pack that could allow arbitrary code execution were discovered and fixed.
US-CERT, "Vulnerability Note VU#380039 Ruby on Rails Action Pack framework insecurely typecasts YAML and Symbol XML parameters" (http://www.kb.cert.org/vuls/id/380039).

10

11 **V** **9th:** Microsoft published their Security Bulletin Summary for January 2013, and released two critical and five important updates.
"Microsoft Security Bulletin Summary for January 2013" (http://technet.microsoft.com/en-us/security/bulletin/ms13-jan).

12 **S** **9th:** The official Debian and Python Wiki servers were compromised through the exploit of several known vulnerabilities in MoinMoin.
Debian made the following announcement. "wiki. debian. org security breach"(http://lists.debian.org/debian-devel-announce/2013/01/msg00000.html).

13 **V** **14th:** Oracle released an unscheduled update for the Java SE JDK and JRE related to unpatched vulnerabilities that could allow arbitrary code execution, which were disclosed on January 11.
"Oracle Security Alert for CVE-2013-0422" (http://www.oracle.com/technetwork/topics/security/alert-cve-2013-0422-1896849.html).

14

15 **S** **14th:** A number of DoS attacks and website alterations targeting MIT and thought to have been perpetrated by Anonymous occurred.
The Tech, "Anonymous hacks MIT" (http://tech.mit.edu/V132/N61/anonymous.html).

16 **V** **15th:** Microsoft released an unscheduled update related to a publicly disclosed vulnerability affecting Internet Explorer versions 6 through 8 that could allow unauthorized termination and remote arbitrary code execution.
"Microsoft Security Bulletin MS13-008 - Critical: Security Update for Internet Explorer (2799329)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-008).

17

18 **V** **16th:** Oracle released their quarterly scheduled update, which fixed a total of 86 vulnerabilities in multiple products such as Oracle and MySQL.
"Oracle Critical Patch Update Advisory - January 2013" (http://www.oracle.com/technetwork/topics/security/cpujan2013-1515902.html).

19 **O** **18th:** The Telecom Information Sharing and Analysis Center Japan (Telecom-ISAC Japan) hosted a cyber attack exercise, which was attended by telecommunications carriers and critical infrastructure providers.

20 **V** **24th:** It was announced that multiple Barracuda Networks appliances were configured with undisclosed accounts used for support purposes. It also came to light that it was possible to log into these accounts using SSH, etc., from specific IP address ranges.
Barracuda Labs Internet Security Blog,"System Accounts and Remote Access on Barracuda Networks Appliances" (https://www.barracuda.com/blogs/labsblog?bid=3118).

21

22 **S** **25th:** Domain hijackings were carried out using an SQL injection vulnerability in the management screen of the nic.tm ccTLD registry for Turkmenistan.

23 **O** **25th:** US-CERT issued a warning regarding the occurrence of DDoS attacks exploiting CMS that had not been properly updated.
"Alert (TA13-024A) Content Management Systems Security and Associated Risks" (http://www.us-cert.gov/cas/techalerts/TA13-024A.html).

24

25 **S** **26th:** Anonymous carried out Operation Last Resort, altering the website for the United States Sentencing Commission (www.ussc.gov).

26 **S** **28th:** An SQL injection vulnerability in the management screen for the nic.lk ccTLD registry for Sri Lanka led to the leak of approximately 10,000 pieces of account information, including email addresses.

27 **S** **29th:** Twitter published their Transparency Report, which summarized the status of requests for the disclosure of user information from government institutions around the world between July and December, 2012.
"Twitter Transparency Report v2" (http://blog.twitter.com/2013/01/twitter-transparency-report-v2.html).

28 **V** **30th:** Vulnerabilities that could allow arbitrary code execution through the processing of specially crafted SSDP requests by a function in Portable SDK for UPnP were discovered and fixed in a number of products.
US-CERT, "Vulnerability Note VU#922681: Portable SDK for UPnP Devices (libupnp) contains multiple buffer overflows in SSDP" (http://www.kb.cert.org/vuls/id/922681).

29

30 **O** **31st:** IPA published a report that evaluated and summarized the risks of cloud outages as well as measures for avoiding them.
"'The Reliability Demanded from the Cloud as Social Infrastructure and Service Continuity Requirements' report - arrangement and proposal of issues such as avoiding the risk of cloud outages and migrating between data centers - "
(http://www.ipa.go.jp/about/technicalwatch/20130131.html) (in Japanese).

31

[Legend] **V** Vulnerabilities **S** Security Incidents **P** Political and Social Situation **H** History **O** Other

*Dates are in Japan Standard Time

a warning calling for configurations to be revised, reasoning that open DNS resolvers could continue to be used in DNS amplification attacks in the future.

This kind of DNS resolution function is sometimes also provided as a network device function for the broadband routers used by individuals, as well as for the DNS servers set up by regular ISPs, etc. Because this sort of device could also be used in attacks depending on the configuration, organizations including the Open DNS Resolver Project*12, JPCERT/CC*13, and JPRS*14 issued alerts urging for confirmation that DNS resolvers could not be used via the Internet without permission.

Figure 2 shows the IP addresses for senders of 53/UDP communications coming into our honeypots for the current survey period classified by country. It was reported that attacks on Spamhaus took place between March 18 and 22, but no communications fitting the pattern of an attack were detected during this period. However, we can confirm that communications from IP addresses in Canada rose sharply between March 15 and 18. These communications appear to be from IP addresses assigned to two specific providers in Canada, but from the content of the communications we know these were attempted DNS amplification attacks targeting these two IP addresses. This kind of DNS amplification attack has already been made on other attack targets, so ample care must be taken.

■ Attacks and Virus Infections at Government Agencies

A number of attacks on government agencies once again become a topic of discussion during this period. In January, it was reported that the PC of an employee at the Ministry of Agriculture, Forestry and Fisheries had been infected with a computer virus, and a number of pieces of confidential information may have leaked. Some time has passed since this incident occurred, but because it is possible that information was leaked, a commission of inquiry consisting of outside experts such as information security specialists was established, and an investigation is underway*15. Outside specialists were also brought in after suspicious communications were detected between a PC at the Ministry of Foreign Affairs and an external server on the Internet, and it was announced that the details of the corresponding information leak would be analyzed. The National Information Security Center (NISC) provided information for the investigation of the incident at the Ministry of Foreign Affairs.

The results of an investigation into the possibility that rocket-related information was leaked when the PC of an employee at the Japan Aerospace Exploration Agency (JAXA) was infected with a virus in November 2012 were published. They indicated that the infection route was through fraudulent email, and that communications with a malicious external site took place between March 17, 2011 and November 21, 2012. The report also maintained that the infected PC did not handle any sensitive information during the period of infection.

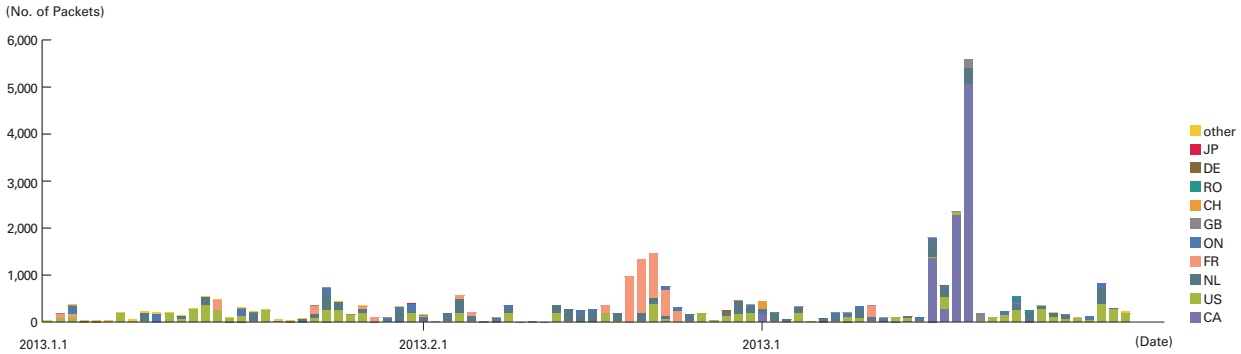


Figure 2: 53/UDP Communications Arriving at Honeypots (by Date, by Country)

*12 Open DNS Resolver Project (http://openresolverproject.org).
*13 JPCERT/CC, "JPCERT/CC Alert 2013-04-18 DDoS attacks using recursive DNS requests" (http://www.jpcert.or.jp/english/at/2013/at130022.html).
*14 JPRS, "Regarding 'Open Resolver' Inappropriate DNS Server Settings" (http://jprs.jp/important/2013/130418.html) (in Japanese).
*15 Ministry of Agriculture, Forestry and Fisheries, "Regarding the Establishment of an Investigative Committee for Cyber Attacks on the Ministry of Agriculture, Forestry and Fisheries, and the 1st Convening of the Committee" (http://www.maff.go.jp/j/press/kanbo/hisyo/130111.html) (in Japanese).

February Incidents

1 V **2nd:** Oracle released an unscheduled update for Java SE JDK and JRE that fixed a total of 50 vulnerabilities after attacks targeting unpatched vulnerabilities were observed.
"Oracle Java SE Critical Patch Update Advisory - February 2013" (http://www.oracle.com/technetwork/topics/security/javacpufeb2013-1841061.html).

2 S **2nd:** Twitter announced they had initiated a forced reset of passwords for the accounts of approximately 250,000 users whose information may have been accessed without authorization.
Twitter blog,"Keeping our users secure" (https://blog.twitter.com/2013/keeping-our-users-secure).

3

4 S **4th:** A suspect was arrested by the Fukuoka Prefectural Police for allegedly violating the Unauthorized Computer Access Law and the Unfair Competition Prevention Act (Infringement Upon Trade Secrets) by accessing a rival company's servers without authorization and obtaining trade secrets.

5 S **5th:** An incident occurred in which access to major media sites hosting advertisements from an advertisement provider was blocked in browsers such as Google Chrome. This was caused by a malware infection at the advertising provider, which led to it being added to blacklists.
See the following Kaspersky Lab Threatpost for more information. "Google Blocks High Profile Sites After Advertising Provider NetSeer is Hacked" (http://threatpost.com/google-blocks-high-profile-sites-after-advertising-provider-netseer-hacked-020413/).

6 S **5th:** The Ministry of Foreign Affairs announced that a PC at the ministry had been infected by a virus, and it suspected approximately 20 documents had leaked to external servers on the Internet.
"Leakage of Information from the MOFA Network to the Internet" (http://www.mofa.go.jp/announce/announce/2013/2/0205_03.html).

7

8 O **6th:** The Tokyo District Court issued a provisional ruling ordering a U.S. Web service provider to disclose the details of a user thought to have made libelous comments. The Civil Proceedings Act was amended in 2011, making it applicable to foreign corporations recognized to be conducting business in Japan.

9 S **7th:** Microsoft's Digital Crime Unit (DCU) and Symantec announced they had launched a joint takedown of the Bamital botnet.
The Official Microsoft Blog, "Microsoft and Symantec Take Down Bamital Botnet That Hijacks Online Searches"
(http://blogs.technet.com/b/microsoft_blog/archive/2013/02/06/microsoft-and-symantec-take-down-bamital-botnet-that-hijacks-online-searches.aspx).

10 O **8th:** A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB13-04: Security updates available for Adobe Flash Player" (http://www.adobe.com/support/security/bulletins/apsb13-04.html).

11 S **10th:** The suspect in the "Remote Control Virus" incident was arrested on suspicion of forcible obstruction of business.

12 S **12th:** An incident of domain hijacking by an unknown party occurred at the Malawi (.mw) ccTLD registry.

13 V **13th:** Microsoft published their Security Bulletin Summary for February 2013, and released five critical updates including MS13-009 and MS13-010, as well as seven important updates.
"Microsoft Security Bulletin Summary for February 2013" (http://technet.microsoft.com/en-us/security/bulletin/ms13-feb).

14 V **13th:** A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB13-05: Security updates available for Adobe Flash Player" (http://www.adobe.com/support/security/bulletins/apsb13-05.html).

15

16

17 O **18th:** The University of Oxford temporarily blocked access to Google Docs as a measure against an increase in phishing incidents exploiting the service. As this had a major impact on users, the measure was cancelled within a few hours.
See the following OxCERT's blog post, "Google Blocks," for more information (http://blogs.oucs.ox.ac.uk/oxcert/2013/02/18/google-blocks/).

18 O **18th:** CERT Australia published its annual report, summarizing incidents such as cyber attacks and crime in 2012 based on corporate surveys. This report presented a number of details, such as the fact that 44% of the companies that responded had experienced an attack from within their organization.
"The Cyber Crime and Security Survey Report" (https://www.cert.gov.au/system/files/608/673/Cyber%20Crime%20and%20Security%20Survey%20Report%202012.pdf).

19 S **19th:** The Japan Aerospace Exploration Agency (JAXA) published the results of its investigation into the virus infection there in November of last year. The infection was caused by the opening of an attachment in a fraudulent email regarding the Great East Japan Earthquake.
"Investigation Result of JAXA Computer Virus Infection Incident" (http://www.jaxa.jp/press/2013/02/20130219_security_e.html).

20 V **20th:** Oracle released a scheduled update for Java SE JDK and JRE that fixed a total of five vulnerabilities.
"Updated Release of the February 2013 Oracle Java SE Critical Patch Update"
(http://www.oracle.com/technetwork/topics/security/javacpufeb2013update-1905892.html).

21 S **20th:** The EDUCAUSE .edu domain registry announced that the information of approximately 90,000 users and 7000 .edu domain owners may have been leaked in a security breach.
"EDUCAUSE SECURITY BREACH AND PASSWORD CHANGE INFORMATION"
(http://www.educause.edu/educause-security-breach-and-password-change-information).

22 O **20th:** Mandiant published a detailed report regarding a series of attacks made over several years targeting companies and organizations in the United States.
"APT1: Exposing One of China's Cyber Espionage Units" (http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf).

23 V **21st:** A number of vulnerabilities in Adobe Reader and Acrobat that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB13-07: Security updates available for Adobe Reader and Acrobat" (http://www.adobe.com/support/security/bulletins/apsb13-07.html).

24 S **22nd:** Twitter announced it would use DMARC (Domain-based Message Authentication, Reporting and Conformance) as a phishing countermeasure.
Twitter blog, "Introducing DMARC for Twitter.com emails" (https://blog.twitter.com/2013/introducing-dmarc-twittercom-emails).

25 V **26th:** A vulnerability in JustSystems Corporation's Ichitaro and Hanako software products that could allow arbitrary code execution was discovered and fixed.
"[JS13001] Regarding the Risk of Malicious Program Execution Exploiting a Vulnerability in Ichitaro and Hanako"
(http://www.justsystems.com/jp/info/js13001.html?m=jui26j03) (in Japanese).

26

27 V **27th:** A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB13-08: Security updates available for Adobe Flash Player" (http://www.adobe.com/support/security/bulletins/apsb13-08.html).

28

[Legend] V Vulnerabilities | S Security Incidents | P Political and Social Situation | H History | O Other

*Dates are in Japan Standard Time

Additionally, a number of incidents of fraudulent email and website alterations occurred. A warning was issued regarding fraudulent email appearing to be from a Ministry of Defense employee*16, and websites operated by the Ministry of the Environment*17 and the National Institute for Agro-Environmental Sciences*18 were altered, along with websites of the High Energy Accelerator Research Organization (KEK)*19 and a number of local public bodies. Of these, in several cases the altered websites were used as stepping stones in attacks or to direct users to malicious websites.

■ Attacks on CMS and Web Servers

During the current survey period, attacks on CMS (Content Management Systems) received widespread attention. In January, US-CERT issued an alert regarding the use of CMS. This alert called for proper management of these systems, such as upgrading the software, indicating that attacks were focused on the open source CMS Joomla! in particular, and compromised servers were being used in DDoS attacks on critical infrastructure companies, etc.

There were also reports of alterations using malicious Web server (Apache) modules, with a large number of cases in Japan whereby malicious Apache modules were placed on Web servers, and JavaScript inserted without users' knowledge when websites were viewed. When users viewed an altered website, they could be redirected to another malicious website and infected with malware. The JPCERT Coordination Center issued a warning about altered websites, indicating that many old versions of server management tools were in use, including those that were no longer supported*20. See "1.4.2 Website Alterations and Drive-By Download Attacks in Japan" for more information about these issues.

■ Attacks on TLD

Attacks on domain registries including ccTLD continue to occur, along with associated domain hijackings and information leaks. In January, domain hijackings occurred after the nic.tm registry that manages the .tm domains for Turkmenistan was the target of an SQL injection attack. A total of 10,000 pieces of account information were also leaked due to an SQL injection attack at the LK Domain Registry that manages the .lk domains for Sri Lanka. In February, there were hijackings of Malawi .mw domains. In the same month, the servers of Pakistan .pk domain registrar PKNIC were compromised, leading to domain hijackings. A similar incident occurred for .pk in November 2012. In these incidents, domain hijackings targeted the regional domains for global companies such as Google or PayPal.

■ Targeted Attacks Seeking Confidential Information

In February, U.S. security firm Mandiant published a detailed report regarding targeted attacks that had been made on U.S. companies and organizations over a period of several years. Around this same time, there was a series of announcements regarding attacks on a number of companies, such as Facebook*21 and Microsoft*22. US-CERT issued an alert due to this malicious activity targeting U.S. government institutions and private sector companies*23. Outside the U.S., there have also been reports of this kind of activity in the EU defense industry, and attacks on a number of ministries and private-sector businesses in Japan have occurred on a continual basis since they began making news in 2011. These incidents have targeted confidential information at general companies in addition to defense industry companies and government agencies, and we believe that similar attacks will continue in the future.

■ The "Remote Control Virus"

During the current survey period, there was a lot of interest in a series of incidents related to the "Remote Control Virus," which came into prominence in October of last year. On January 1 and January 5, messages purporting to be quizzes from the supposed perpetrator of the virus were sent by email to a number of media outlets and reporters. Two locations were

*16 Ministry of Defense, "Beware of 'Fraudulent Email' Appearing to be From Employees of the Ministry of Defense" (http://www.mod.go.jp/j/approach/others/security/narisumashi.html) (in Japanese).
*17 Ministry of the Environment, "(Notice) Regarding the Alteration of the 'CO2 Mieru Tool' Site" (http://www.env.go.jp/info/mieeeru.pdf) (in Japanese).
*18 National Institute for Agro-Environmental Sciences, "Regarding Unauthorized Access to the National Institute for Agro-Environmental Sciences Website" (http://www.niaes.affrc.go.jp/techdoc/press/130122/press130122.html) (in Japanese).
*19 High Energy Accelerator Research Organization(KEK), "Defacing incident on the website of the KEK Theory Center" (http://legacy.kek.jp/intra-e/info/2013/032217/).
*20 JPCERT/CC, "JPCERT/CC Alert 2013-04-08 Alert regarding the usage of old versions of Parallels Plesk Panel" (http://www.jpcert.or.jp/english/at/2013/at130018.html).
*21 Facebook, "Protecting People On Facebook" (https://www.facebook.com/notes/facebook-security/protecting-people-on-facebook/10151249208250766).
*22 Microsoft Security Response Center, "Recent Cyberattacks" (http://blogs.technet.com/b/msrc/archive/2013/02/22/recent-cyberattacks.aspx).
*23 US-CERT, "UPDATE: Ongoing Malicious Cyber Activity Against U. S. Government and Private Sector Entities" (http://www.us-cert.gov/ncas/current-activity/2013/02/22/Ongoing-Malicious-Cyber-Activity-Against-US-Government-and-Private).

March Incidents

1 2 **O** **1st:** The Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry published an amended version of the "List of Recommendable Cryptographic Techniques for Procurement Activities by Japan e-Government (CRYPTREC Ciphers List)" that was drawn up in 2003.
CRYPTREC, "CRYPTREC Ciphers List (Japan e-Government Recommendable Cryptographic Techniques List)" (http://www.cryptrec.go.jp/list.html) (in Japanese).

3 4 **S** **3rd:** Evernote announced that it had reset all user passwords due to an incident in which user information was accessed.
"Security Notice: Service-wide Password Reset" (http://blog.evernote.com/blog/2013/03/02/security-notice-service-wide-password-reset/).

5 **V** **5th:** Oracle released an unscheduled update for Java SE JDK and JRE that fixed a number of vulnerabilities, including one that allowed arbitrary code execution (CVE-2013-1493).
"Oracle Security Alert for CVE-2013-1493" (http://www.oracle.com/technetwork/topics/security/alert-cve-2013-1493-1915081.html).

6 **S** **5th:** Access to a number of sites in Japan was blocked by Google Safe Browsing in multiple browsers including Google Chrome.

7 8 **O** **8th:** The JPCERT Coordination Center announced the establishment of the "ConPaS (Control System Security Partner's Site)" information sharing portal site for facilitating the circulation of information on dealing with security threats to control systems.
"Regarding the Portal Site for Sharing Information on Control System Security Threats" (http://www.jpcert.or.jp/ics/conpas/index.html) (in Japanese).

9 10 **S** **9th:** Sites such as the vulnerability information database of the National Institute of Standards and Technology (NIST) in the U.S. ceased operation due to malware infections caused by a Web server vulnerability.
See the following post to Google+ from a security expert for more information about this incident. Kim Halavakoski, "http://nvd.nist.gov/ hacked. Site down since March 8..." (https://plus.google.com/u/0/106350285372295328202/posts/HNayDzUoYEz).

11 12 **O** **12th:** The IPA published "10 Major Security Threats for 2013 - Threats Looming Close".
"'10 Major Security Threats for 2013 - Threats Looming Close' Published" (http://www.ipa.go.jp/about/press/20130312_2.html) (in Japanese).

13 **V** **13th:** Microsoft published their Security Bulletin Summary for March 2013, and released four critical updates including MS13-021, as well as three important updates.
"Microsoft Security Bulletin Summary for March 2013" (http://technet.microsoft.com/en-us/security/bulletin/ms13-mar).

14 15 **V** **13th:** A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB13-09: Security updates available for Adobe Flash Player" (http://www.adobe.com/support/security/bulletins/apsb13-09.html).

16 17 **S** **15th:** It was reported that a number of websites in Japan had been altered with the installation of malicious Apache modules and used in attacks. The JPCERT Coordination Center issued a warning regarding this incident on April 8, indicating that many of the altered websites had used old versions of Parallels Plesk Panel.
"JPCERT/CC Alert 2013-04-08 Alert regarding the usage of old versions of Parallels Plesk Panel" (http://www.jpcert.or.jp/english/at/2013/at130018.html).

18 19 **S** **18th:** A large-scale DDoS attack was made on Spamhaus, as well as CloudFlare after it joined efforts to cope with the attack.
See the following CloudFlare blog post for details regarding this incident. "The DDoS That Almost Broke the Internet" (http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet).

20 21 **O** **19th:** The "Internet Census 2012" was published, summarizing the results of a survey in which the Internet IP address space was scanned. Approximately 420,000 devices with security issues were used in the survey for this census, which states that a total of over two million connected devices had security issues. This census demonstrates that many insecure devices are connected to the Internet.
"Internet Census 2012" (http://internetcensus2012.bitbucket.org/paper.html).

22 23 **S** **20th:** Attacks involving malware were made on major broadcasting stations and financial institutions in South Korea. This led to the destruction of hard drive data on approximately 47,800 PCs and servers, and put ATMs and online banking services out of action.

24 **S** **22nd:** The suspect arrested for the "Remote Control Virus" incident was charged with a number of crimes, including forcible obstruction of business.

25 **O** **25th:** The IPA published its "Guidelines for Preventing Insider Threats at Organizations," which indicated specific measures for implementing effective provisions against insider threats.
"Guidelines for Preventing Insider Threats at Organizations Published" (http://www.ipa.go.jp/about/press/20130325.html) (in Japanese).

26 27 **V** **26th:** A vulnerability (CVE-2013-2266) in BIND 9.7 and later that allowed servers to be terminated was discovered and fixed.
Internet Systems Consortium, "CVE-2013-2266: A Maliciously Crafted Regular Expression Can Cause Memory Exhaustion in named" (https://kb.isc.org/article/AA-00871/74/CVE-2013-2266%3A-A-Maliciously-Crafted-Regular-Expression-Can-Cause-Memory-Exhaustion-in-named.html).

28 29 **S** **26th:** A failure occurred, preventing the basic resident register network system (Juki Net) from being used at 231 local authorities in Japan.
The Ministry of Internal Affairs and Communications published the results of their investigation on April 2, indicating that an error in the text encoding of data was to blame. "Regarding the System Failure at local municipality Juki Net CS" (http://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000130.html) (in Japanese).

30 31 **O** **30th:** US-CERT issued a warning urging that settings for public DNS servers be reconfigured due to the possibility of them being used in DNS amplification attacks.
"Alert (TA13-088A) DNS Amplification Attacks" (http://www.us-cert.gov/ncas/alerts/TA13-088A).

[Legend] **V** Vulnerabilities **S** Security Incidents **P** Political and Social Situation **H** History **O** Other

*Dates are in Japan Standard Time

identified from the answers to these quizzes, and in one of these locations a cat was found wearing a collar to which a memory card containing data related to the incidents was attached. The collar was subsequently retrieved. On February 10, an individual was arrested on suspicion of forcible obstruction of business. In March the suspect was charged with a number of crimes, including forcible obstruction of business, but he denies the accusations at the time of writing.

■ Efforts to Implement Security Measures at Government Institutions

Recent developments in security measures at government institutions include the amendment of the CRYPTREC Ciphers List (List of Recommendable Cryptographic Techniques for Procurement Activities by Japan e-Government), which has been used as a unified management standard for information security measures at government institutions. The original list was intended for use over a period of about 10 years due to concerns about the compromise of cryptographic algorithms through advancements in analysis and attack technology. For this reason, work on amendments was made over a span of four years from 2009. The amendments resulted in the definition of three lists: the "e-Government Recommended Ciphers List," the "Recommended Candidates Ciphers List," and the "Operational Monitoring Ciphers List." The Information Security Policy Council is also discussing the establishment of a new basic strategy for information security to replace the "Information Security Strategy to Protect Citizens" established in 2010*24*25.

■ Other

In February, the Tokyo District Court issued a provisional ruling ordering a U.S. Web service provider operating in Japan to disclose the details of a user thought to have made libelous comments. This was possible due to amendments to the Civil Proceedings Act in 2011 that made it applicable to foreign corporations recognized to be conducting business in Japan.

In the same month, a number of major media sites hosting advertisements from a U.S. advertising provider were labeled as containing malicious software through the Google Safe Browsing function, making it impossible to access them from browsers such as Chrome. This was because the advertising provider's domain had been added to blacklists after it was infected with malware. The advertisement distribution system was subsequently not found to be infected, so access to the sites was soon restored. Similar incidents also affected multiple websites in March, including those for major media outlets in Japan. These were also triggered by Google Safe Browsing, but the reason for their blocking is not known. An incident in which an advertising distribution service was altered to redirect users of many well-known website to malware infection sites also occurred in Japan in 2010.

Attacks on online sites such as SNS also became a topic of discussion when their authentication information was targeted to exploit stolen IDs and passwords in attempts to steal accounts for other sites. Twitter was attacked in February, and announced they had reset the passwords of some 250,000 users whose user information, including user names, email addresses, and encrypted passwords, may have been accessed. A similar incident occurred at Evernote in March, and the passwords of 50,000,000 Evernote users were reset. The passwords affected in these incidents were encrypted, but measures were taken to improve security.

In March, a number of broadcasting stations and financial institutions in South Korea experienced simultaneous system outages due to malware infections. Tens of thousands of computers were infected in this incident, which led to serious hindrances such as ATMs being rendered inoperable. See "1.4.1 The 3.20 Cyber Attack in South Korea" for more information about this incident.

*24 National Information Security Center, "Information Security Policy Council - 32nd Assembly" (February 22, 2013) (http://www.nisc.go.jp/conference/seisaku/index.html#seisaku32) (in Japanese).

*25 National Information Security Center, "Information Security Policy Council - 33rd Assembly" (March 26, 2013) (http://www.nisc.go.jp/conference/seisaku/index.html#seisaku33) (in Japanese).

1.3 Incident Survey

1.3.1 DDoS Attacks

Today, DDoS attacks on corporate servers are almost a daily occurrence, and the methods involved vary widely. However, most of these attacks are not the type that utilizes 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 3 shows the circumstances of DDoS attacks handled by the IIJ DDoS Defense Service between January 1 and March 31, 2013.

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, and the capacity of the environment attacked (bandwidth and server performance) will largely determine the degree of impact. Figure 3 categorizes DDoS attacks into three types: attacks on bandwidth capacity*26, attacks on servers*27, 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 565 DDoS attacks. This averages to 6.26 attacks per day, indicating a decrease in the average daily number of attacks compared to our prior report. Server attacks accounted for 91.5% of all incidents, and compound attacks accounted for the remaining 8.5%. There were no bandwidth capacity attacks.

The largest attack observed during the period under study was classified as a server attack, and resulted in 228 Mbps of bandwidth using up to 44,000 pps packets.

Of all attacks, 74.2% ended within 30 minutes of commencement, 25.1% lasted between 30 minutes and 24 hours, and 0.7% lasted over 24 hours. The longest sustained attack was a server attack that lasted for one day, 13 hours, and 29 minutes (37 hours and 29 minutes). 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*28 and botnet*29 usage as the method for conducting DDoS attacks.

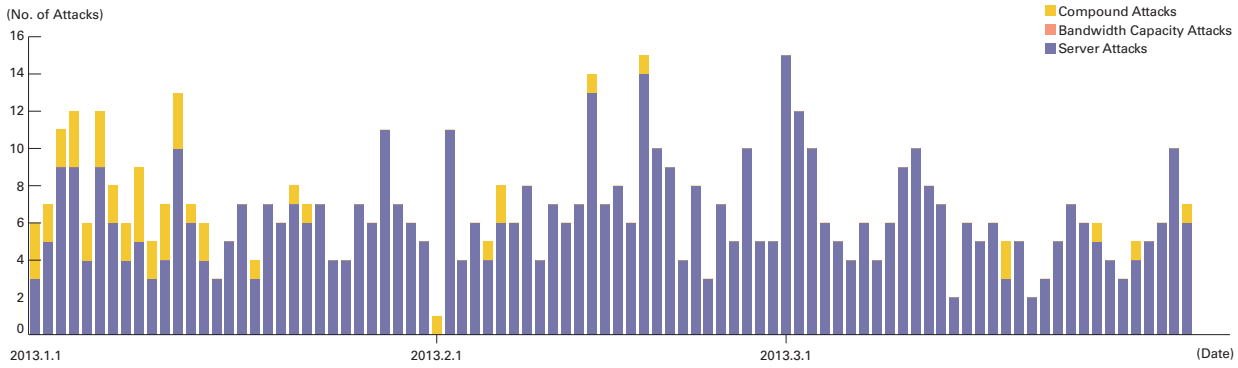


Figure 3: Trends in DDoS Attacks

*26 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.

*27 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.

*28 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 to make it appear as if the attack is coming from a different location, or from a large number of individuals.

*29 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.

■ Backscatter Observations

Next we present our observations of DDoS attack backscatter using the honeypots*30 set up by the MITF, a malware activity observation project operated by IIJ*31. By monitoring backscatter it is possible to detect some of the DDoS attacks occurring on external networks as a third party without any interposition.

For the backscatter observed between January 1 and March 31, 2013, Figure 4 shows the sender's IP addresses classified by country, and Figure 5 shows trends in packet numbers by port. The port most commonly targeted by the DDoS attacks observed was the 80/TCP port used for Web services, accounting for 38.7% of the total during the target period. Attacks were also observed on 6667/TCP used for IRC (Internet Relay Chat), 22/TCP used by SSH, and 25565/TCP, which is thought to be game-related.

Regarding particularly large number of backscatter packets observed, there were many attacks on Web servers (80/TCP) that targeted a number of servers for a DDoS defense service provider in the United States. There were a large number of attacks on IRC (6667/TCP) between February 11 and 17. These attacks targeted the game-related servers of a hosting provider in the U.S. Over 250,000 attacks were observed during a period of six days, excluding February 15. Attacks were also observed on SSH (22/TCP), 25565/TCP, and 7777/TCP, targeting the servers of hosting providers in countries such as the United States, Germany, France, Switzerland, China, Russia, and Kazakhstan.

Notable DDoS attacks during the current survey period that were detected via IIJ's observations of backscatter included attacks on a number of U.S. bank sites thought to be part of Operation Ababil, continued attacks on a religious group that exhibits radical behavior, and attacks on multiple Torrent sites in January. In the same month attacks on a number of MIT sites thought to have been perpetrated by Anonymous took place. Aside from this, Anonymous was thought to be responsible for attacks on several government-related sites in Israel, including its intelligence agency. Attacks were made on a security expert's site in March, and in the same month backscatter was observed from attacks on multiple right-wing political sites in Italy, which are also attributed to Anonymous.

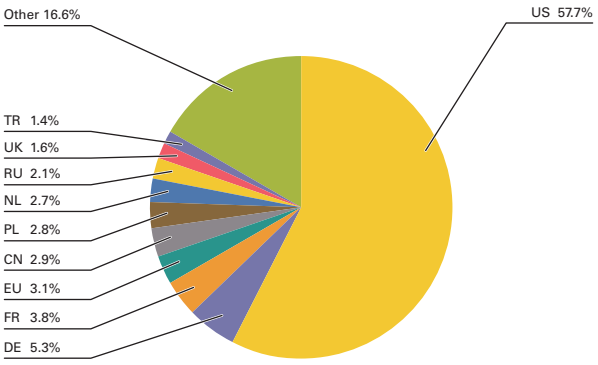


Figure 4: Distribution of DDoS Attack Targets According to Backscatter Observations (by Country, Entire Period under Study)

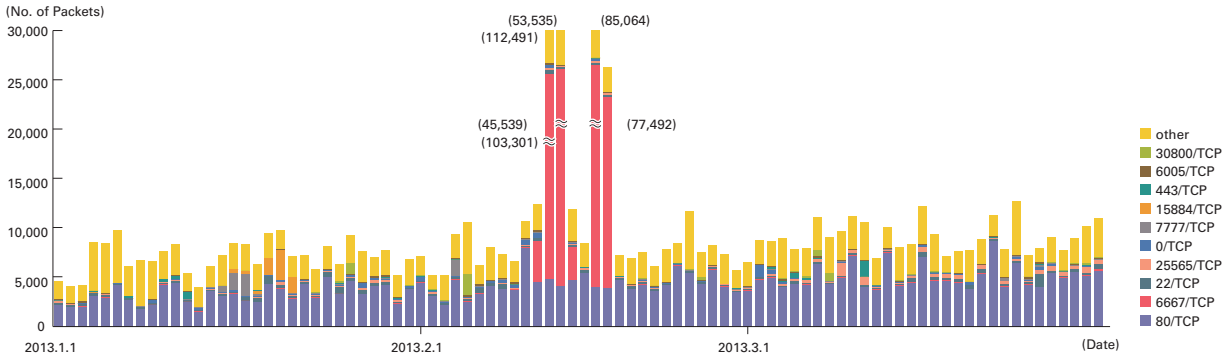


Figure 5: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)

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

*31 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 (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol08_EN.pdf) under "1.4.2 Observations on Backscatter Caused by DDoS Attacks."

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the MITF*32, a malware activity observation project operated by IIJ. The MITF uses honeypots*33 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 the distribution of sender's IP addresses by country for communications coming into the honeypots between January 1 and March 31, 2013. Figure 7 shows trends in the total volumes (incoming packets). The MITF has set up numerous honeypots for the purpose of observation. We have taken the average per honeypot, showing the trends for incoming packet types (top ten) over the entire period subject to study. Additionally, in these observations we corrected data to count multiple TCP connections as a single attack when the attack involved multiple connections to a specific port, such as attacks on MSRPC.

Much of the communications arriving at the honeypots demonstrated scanning behavior targeting TCP ports utilized by Microsoft operating systems. We also observed scanning behavior targeting 1433/TCP used by Microsoft's SQL Server, 3389/TCP used by the RDP remote login function for Windows, 22/TCP used for SSH, 23/TCP used for telnet, and ICMP echo requests. Additionally, communications of an unknown purpose were observed on ports not used by common applications, such as 24539/TCP and 3913/UDP.

Communications thought to be SSH dictionary attacks also occurred during the current survey period. For example, concentrated communications was observed coming from IP addresses assigned to China on January 25, between February 12 and February 16, and on March 6 and March 29. The same type of communications was observed coming from India between February 15 and February 16, from Germany and South Korea on February 15, from Thailand on February 16, and from the United States on March 29. Sporadic increases in ICMP echo requests also occurred, mainly in January. On February 16 high volumes of communications to 3193/UDP were seen coming from Iran and Pakistan. The purpose of these is not known, but due to cases of MyDoom variants using this port, and the fact that vulnerabilities have been confirmed in certain applications that conduct communications via this port, we believe these are exploitation attempts.

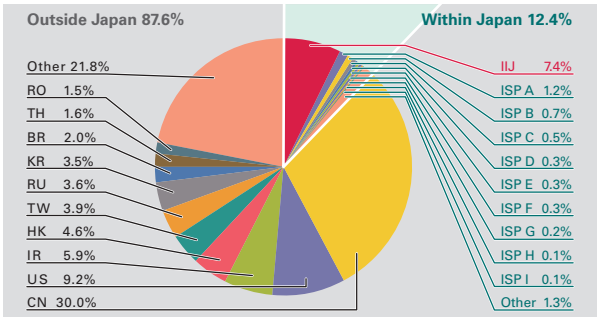


Figure 6: Sender Distribution (by Country, Entire Period under Study)

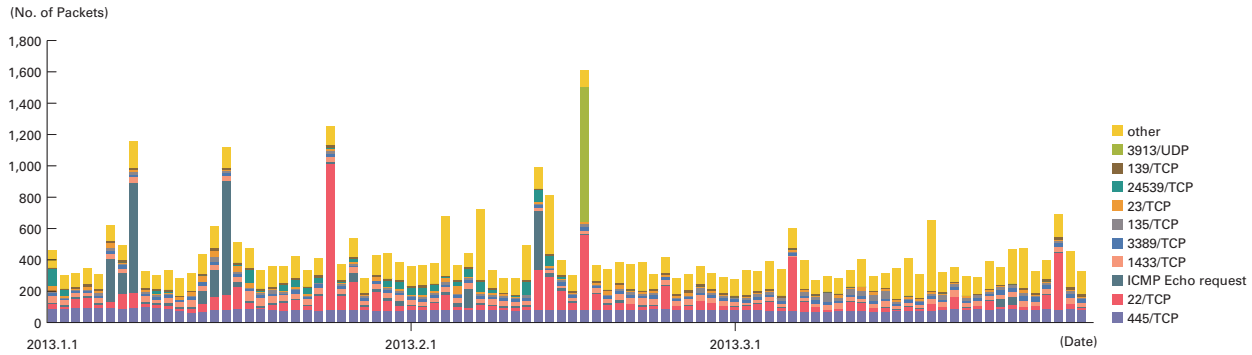


Figure 7: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

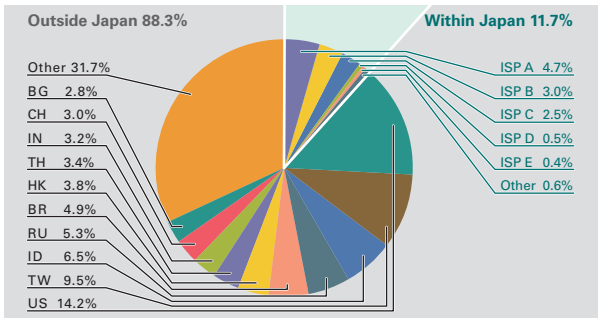
*32 An abbreviation of Malware Investigation Task Force. The Malware Investigation Task Force (MITF) began activities in May 2007, observing malware network activity through the use of honeypots in an attempt to understand the state of malware activities, to gather technical information for countermeasures,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

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

Malware Network Activity

Figure 8 shows the distribution of the specimen acquisition source for malware during the period under study, while Figure 9 shows trends in the total number of malware specimens acquired. Figure 10 shows trends in the number of unique specimens. In Figure 9 and Figure 10, the trends in the number of acquired specimens show the total number of specimens acquired per day*34, while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*35.

Specimens are also identified using anti-virus software, and a breakdown of the top 10 variants is displayed color coded by malware name. As with our previous report, for Figure 9 and Figure 10 we have detected Conficker using multiple anti-virus software packages, and removed any Conficker results when totaling data.



On average, 116 specimens were acquired per day during the period under study, representing 26 different malware. Undetected specimens from Thailand and Indonesia also appeared during the current survey period. After investigating these undetected specimens more closely,

Figure 8: Distribution of the Number of Malware Specimens Acquired

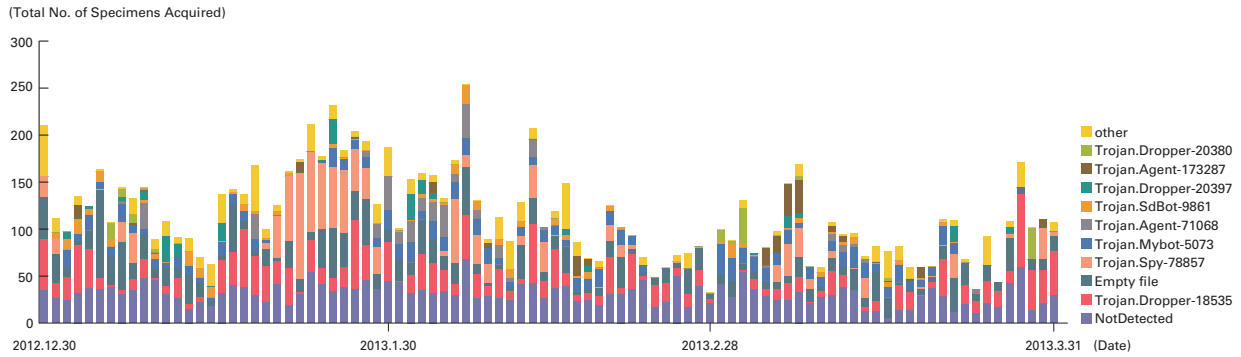


Figure 9: Trends in the Total Number of Malware Specimens Acquired (Excluding Conficker)

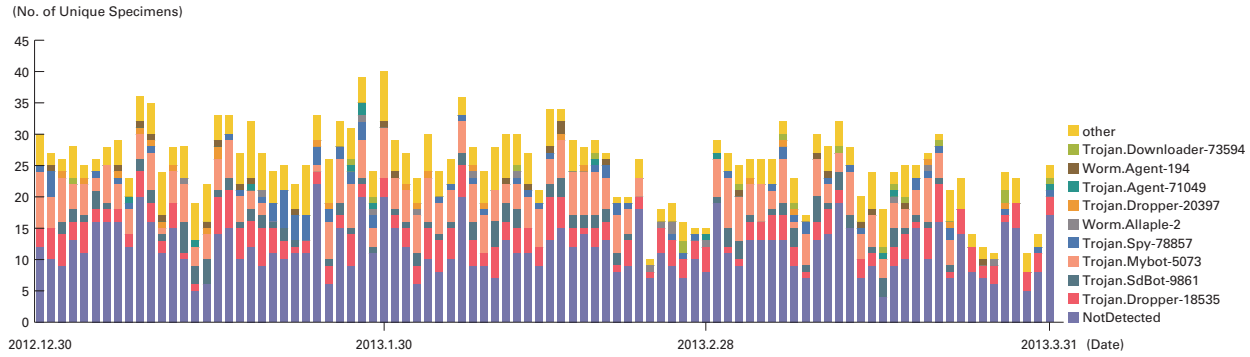


Figure 10: Trends in the Number of Unique Specimens (Excluding Conficker)

*34 This indicates the malware acquired by honeypots.

*35 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.

we learned that two types of bots*36*37 controlled by IRC servers and a ZeuS variant had been active, just as in the past. Worms*38 from IP addresses allocated to the United States and Hong Kong were also observed on an ongoing basis.

Under the MITF's independent analysis, during the current period under observation 73.6% of malware specimens acquired were worms, 21.5% were bots, and 4.9% were downloaders. In addition, the MITF confirmed the presence of 12 botnet C&C servers*39 and 6 malware distribution sites.

Conficker Activity

Including Conficker, an average of 29,256 specimens were acquired per day during the period covered by this report, representing 811 different malware. While figures rise and fall over short periods, Conficker accounts for 99.6% of the total number of specimens acquired, and 96.9% of unique specimens. This demonstrates that Conficker remains the most prevalent malware by far, so we have omitted it from figures in this report.

Comparing the period covered by this report with the previous survey period, the total specimens acquired fell by approximately 30%, and the number of unique specimens fell by approximately 10%. This occurred because the IP addresses of the honeypots used by IIJ for observation fell under the IP address space*40 not targeted by some Conficker variants for infection.

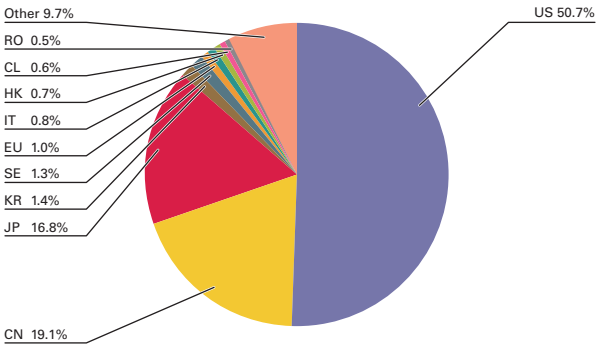


Figure 11: Distribution of SQL Injection Attacks by Source

According to the observations of the Conficker Working Group*41, as of March 31, 2013, a total of 1,497,909 unique IP addresses are infected. This is a drop of approximately 47% compared to the 3.2 million PCs observed in November 2011, but it demonstrates that infections are still widespread.

1.3.3 SQL Injection Attacks

Of the types of different Web server attacks, IIJ conducts ongoing surveys related to SQL injection attacks*42. SQL injection attacks have flared up in frequency numerous times in the past, and remain one of the major topics in

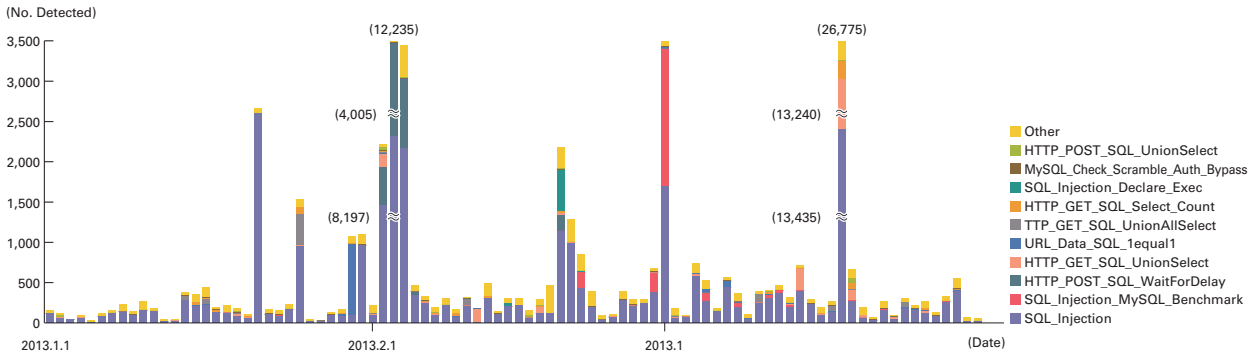


Figure 12: Trends in SQL Injection Attacks (by Day, by Attack Type)

*36 Trojan:Win32/Ircbrute (http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?name=Trojan%3AWin32%2FIrcbrute).
*37 Win32/Hamweq (http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fHamweq).
*38 WORM_DEBORM. AP (http://about-threats.trendmicro.com/Malware.aspx?id=36201&name=WORM_DEBORM.AP&language=au).
*39 An abbreviation of Command & Control Server. A server that provides commands to a botnet consisting of a large number of bots.
*40 The phenomenon of Conficker not targeting certain IP address ranges for infection has been reported on the dionaea developer's blog "Conficker does not like me?" (http://carnivore.it/2009/11/03/conficker_does_not_like_me).
*41 Conficker Working Group Observations (http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking).
*42 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.

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 11 shows the distribution of SQL injection attacks against Web servers detected between January 1 and March 31, 2013. Figure 12 shows trends in the numbers of attacks. These are a summary of attacks detected by signatures on the IIJ Managed IPS Service.

The United States was the source for 50.7% of attacks observed, while China and Japan accounted for 19.1% and 16.8%, respectively, with other countries following in order. There was a dramatic increase in the number of SQL injection attacks against Web servers compared to the previous report.

Attacks from the United States rose to first place, and those from China rose to 2nd place, due to large-scale attacks directed at specific targets that occurred on certain days. Japan dropped to third highest, but the number of attacks increased compared to the previous survey period.

During this period, attacks from a specific attack source in Japan directed at specific targets took place on January 21. Between February 3 and 4, attacks were made from a specific attack source in China against specific targets. On March 1, a large-scale attack from a specific attack source in the United States was made on specific targets. A number of specific attack sources in the United States also made large-scale attacks directed at specific targets on March 18. These attacks are thought to have been attempts to find vulnerabilities on a Web server.

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

1.4 Focused Research

Incidents occurring over the Internet change in type and scope from one minute to the next. Accordingly, IIJ works toward implementing countermeasures by continuing to perform independent surveys and analyses of prevalent incidents. Here we will present information from the surveys we have undertaken during this period, including a look at the 3.20 Cyber Attack in South Korea that resulted in issues such as system failures due to mass malware infections in March, as well as an incident in which a large number of websites in Japan were altered and used to redirect users to malicious sites. We will also discuss exercises on responding to the cyber attacks that are being carried out around the world at a brisk pace.

1.4.1 The 3.20 Cyber Attack in South Korea

In the afternoon of March 20, system failures occurred at a number of broadcasting stations and financial institutions in South Korea due to mass simultaneous malware infections. Tens of thousands of computers went down across the six organizations affected, and damages at financial institutions included ATM machines being rendered inoperable. In this section we give an account of the incident as a whole.

■ Malware Behavior

Malware infections were directly responsible for the system failures. The types of malware identified in this incident are known as Dropper and Wiper. Dropper malware is designed to create and execute related programs such as Wiper malware. The Wiper malware overwrites the MBR (Master Boot Record) sector and file system of a hard disk, destroying them. Affected machines are then forced to reboot, but because the MBR is destroyed, the OS does not launch.

IIJ obtained and analyzed specimens of these malware types independently, and found them to have the following characteristics.

Dropper Characteristics

- Creates four files, including Wiper programs for Windows and Unix.
- Checks for the presence of "C:\Windows\Temp\~v3.log", and executes the Windows Wiper file if it does not exist.
- Obtains information such as the host name and root user password from the mRemote or SecureCRT (both SSH client software) configuration file.
- Based on the information obtained, uses SCP to copy the Unix Wiper program to the server, then once again connects via SSH and executes it.

Windows Wiper Characteristics

- Checks for the presence of "C:\Windows\Temp\~v3.log", and ends without doing anything if it exists (some variants do not perform this check).
- Waits until the local time is 2:00 PM on March 20 (some variants do not wait).
- Uses the taskkill command to stop pasvc.exe (AhnLab Policy Agent) and clisvc.exe (Hauri ViRobot ISMS).
- Overwrites the MBR and the first sector of each partition with a specific character string, destroying them (some variants use a different character string).
- Overwrites logical drives B through Z from the first sector with a specific character string, destroying them.
- Restarts Windows after five minutes pass.

Unix Wiper Characteristics

- Behavior varies somewhat depending on the OS type (HP-UX, AIX, Solaris, Linux).
- Carries out either or both of the following destructive actions: (1) uses the dd command to overwrite partitions with /dev/null (2) uses the rm command to delete directories.

As mentioned above, there are a number of Wiper variants that exhibit different behavior. We also know from sources such as security vendor reports that there are other variants that IIJ has not been able to obtain*43. Some of these Wiper malware variants begin their destructive activity immediately after infection, but others were designed to execute after 2:00PM or 3:00PM on March 20, and we believe this is the reason that a number of organizations were affected by malware at the same time.

Additionally, because the termination of processes only targeted products from two South Korean security vendors, and checks were only made for the configuration file of specific remote connection tools, we can assume that the malware was tailored to a limited number of targets. If the malware effectively destroyed property at affected organizations on purpose, it is highly likely that the attacker researched the target organizations carefully in advance.

Infection Vectors

Regarding the malware infection vectors, according to a report from the Korean Communications Commission (KCC), malware was distributed to clients from asset management servers deployed at affected organizations*44. These six companies had implemented management products from South Korean security vendors such as AhnLab's AhnLab Policy Center (APC), and Hauri's ViRobot ISMS. Normally, automatic program updates and distribution to clients are carried out using management servers, and in this case it appears this system was used to distribute malware (however, there have also been reports that malware was distributed by a system other than management products of these security vendors at some of the affected organizations).

Put simply, the attacker infiltrated the networks at these organizations ahead of time, and hijacked the asset management server to distribute malware. The method used to break into the asset management server is not clear, but AhnLab reported that the version of APC at one of the affected organizations had a vulnerability that allowed login authentication to be bypassed, which was exploited by the attacker*45.

From these facts, we believe that this attack was conducted in three stages (see Figure 13).

*43 For example, in AhnLab's analysis at least three types of Dropper and four types of Windows Wiper were confirmed. ASEC Threat Research & Response blog: 주요 방송사및 은행 전산망 장애 유발 악성코드 분석 (http://asec.ahnlab.com/926) (in Korean).

*44 According to an announcement from KCC on March 21. 民·官·軍 사이버위협 합동대응팀, 공격 주체 규명에 주력 (http://old.kcc.go.kr/user.do?mode=view&boardId=1042&page=P05030000&dc=K04030000&boardSeq=36096) (in Korean).

*45 According to an announcement from AhnLab on March 29. 안랩, 3.20 전산망 마비 농협관련 자체 중간조사 결과 발표 (http://blog.ahnlab.com/ahnlab/1732) (in Korean).

(1) PCs at affected organization got infected with malware (Initial Infection)
(2) Attacker broke into the asset management servers
(3) Attacker distributed malware to clients from these servers

At this point in time, it is not known how the initial infection in stage one was carried out. A number of security vendors have made educated guesses, bringing up the possibility that infections were caused when an employee at the affected organization opened an email with malware attached, or that PCs were infected with malware when an external website was viewed. However, no official confirmation has been made.

Furthermore, according to reports from the South Korean police, some of the malware was sent from four western countries, and they are requesting cooperation from those countries in the investigation. None of the Dropper and Wiper specimens analyzed by IIJ included functions for external communication. For this reason, we surmise that multiple different types of malware were used.

■ Response in South Korea

The response in South Korea after the incident occurred was comparatively fast, with the President issuing a directive to restore service and ascertain the cause swiftly, and a public-private-military joint response team moving to investigate. A dedicated malware removal tool was also released within the same day through the cooperation of security vendors, and the government provided support to help affected organizations recover*46. As of March 29 the joint response team announced that restoration of affected systems was complete, but the full investigation of the cause and efforts to prevent reoccurrence are expected to take some time.

As a result of this incident, the South Korean government held a "National Cyber Security Strategy Council" on April 11, attended by 15 related organizations centered on the National Intelligence Service. A number of plans were announced as a result, including the drawing up of a "National Cyber Security Package" in the first half of the year, which is to be implemented in the second half. Plans to overhaul related legal systems and promote international cooperation in deterring cyber terrorism by North Korea were also announced*47. It appears that moves to redevelop systems for responding to cyber threats will be accelerated for some time to come.

■ Connection with Past Incidents

There were also incidents in South Korea in July of 2009 and March of 2011 in which approximately 110,000 PCs were infected with malware, and these PCs made DDoS attacks against major sites in South Korea and the United States. The malware used in these cases had functions for destroying the data on hard disks, causing damage to infected PCs.

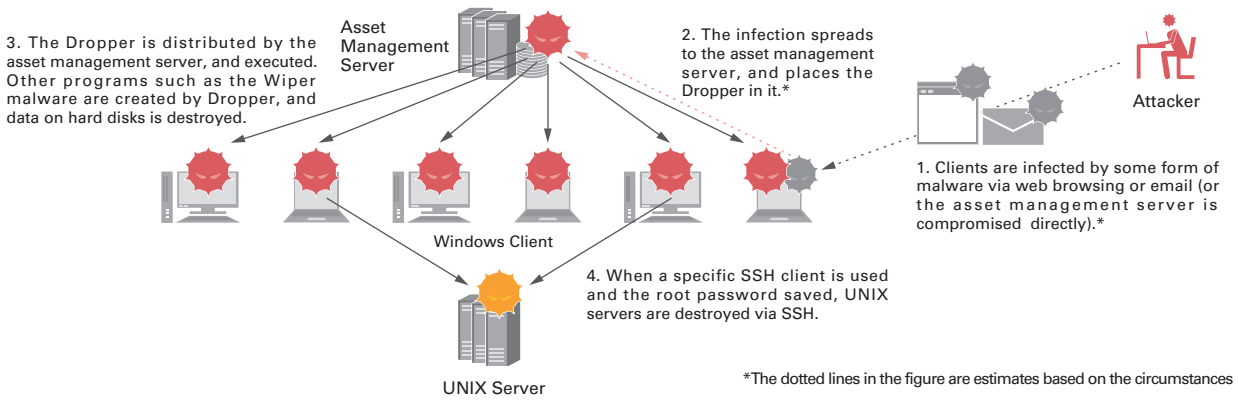


Figure 13: Malware Infection Flowchart

*46 The Korea Internet & Security Agency (KISA) released a removal tool on the Internet on March 21. 방송사 금융사 전산망 마비시킨 악성코드 치료 전용백신 배포 (http://www.boho.or.kr/kor/notice/noticeView.jsp?p_bulletin_writing_sequence=2033) (in Korean).
*47 The Ministry of Science, ICT & Future Planning (MSIP) made an announcement on April 12. '3.20 사이버테러' 관련 국가 사이버안전 전략회의 개최 - 국가사이버안보 종합대책 수립키로 (http://www.msip.go.kr/Board_detailForm.action?bbsId=72&bbsNo=219) (in Korean).

The South Korean government released an interim report regarding the latest incident on April 10, revealing that there was considerable evidence indicating that it was connected to these past incidents*48. According to the report, many of the 76 malware variants and 49 IP addresses that served as relay points in the latest attacks were also used in past attacks. Additionally, it is now known that the attacker broke into the networks of targeted organizations and started making preparations at least eight months in advance.

■ Impact on Japan

Because asset management servers mainly used in South Korea were the origin of the malware distributed in this incident, and specific organizations in South Korea were targeted, other companies, including those in Japan, suffered little immediate effect. On the other hand, we must note that the attack method used in this incident, where malware is distributed from management servers within an organization, could also be used in Japan. Additionally, in targeted attacks in the past we have seen many cases of attackers who have broken into an organization examining the network and attacking authentication servers such as Active Directory. Currently there are many unanswered questions regarding the initial method used to break into the organizations affected by this incident, so specific matters of concern cannot be identified. However, we think that now would be a good time to check the security status of management servers that can control large numbers of PCs.

1.4.2 Website Alterations and Drive-By Download Attacks in Japan

In-mid-March 2013, an article was published on a security researcher's blog*49 stating that 285 websites in Japan had been altered, and visitors were being redirected to malicious servers. IIJ conducted a survey of these 285 sites, as well as a number of other websites suspected of being associated with them, and analyzed the tools and malware used in this series of attacks.

■ Overview of the Attack

■ Altered Websites

The altered websites act as "redirectors" that send visitors to malicious servers and infect them with malware. Specifically, iframe tags that reference a malicious server (infector) are injected into the content browsed by client PCs. In this incident, an Apache module called DarkLeech installed on websites without authorization injected iframe tags into text content such as HTML or JavaScript dynamically. The URLs for the infectors referenced were obtained each time from external C&C servers, with each URL cached for 10 minutes. We discovered that because URLs for the infector were once again obtained from the C&C server after timing out, the infector URL could be changed within short periods of time*50.

■ Malicious Servers Causing Malware Infections

It has been reported that the infectors users were redirected to used BHEK2 (Blackhole Exploit Kit version 2). BHEK2 exploits vulnerabilities in browser plug-ins for software such as Java, Adobe Flash, and Adobe Reader on client PCs in an attempt to infect them with malware. In this case a number of infectors were used, and those IIJ confirmed were mostly run on servers outside Japan, with the vast majority on a node belonging to a certain hosting provider in the United States.

■ Malware Used in Infections

We have confirmed that malware known as Pony was installed when infection via the infector succeeded. However, because it has been reported that BHEK2 had been used to infect clients with a variety of malware other than Pony, such as ZeuS variants (including Citadel) and ZeroAccess, we believe it is possible that these malware types may have also been distributed along with Pony in this incident. Pony steals account information and downloads other malware. IIJ analyzed a Pony specimen obtained on March 15, 2013, and found the version of Pony used to be 1.9. This version featured functions to steal authentication information from almost 100 types of client software, including various Web browsers, mailers, and FTP/SSH/RDP applications*51. It also attempted to steal information for applications mainly used in Japan, such as FFFTP and

*48 The Ministry of Science, ICT & Future Planning (MSIP) made an announcement on April 10. 民官軍 합동대응팀, '3.20 사이버테러' 중간 조사결과 발표 - 북한의 과거 해킹수법과 일치하는 증거 발견 (http://www.msip.go.kr/Board_detailForm.action?bbsId=72&bbsNo=182) (in Korean).

*49 Published on 0day.jp on March 15, 2013 "#OCJP-098: [Warning] 285 websites in Japan are infected with DarkLeech Apache Modules, and users accessing them with IE are redirected to 'Blackhole' malware infection sites" (http://unixfreaxjp.blogspot.jp/2013/03/ocjp-098-285blackhole-exploit-kit.html) (in Japanese).

*50 See "Mass Alterations Using BHEK2" (https://sect.iij.ad.jp/d/2013/03/154955.html) (in Japanese) for more information on trends in attacks and the characteristics of infector URL patterns.

*51 See "Follow-Up on Alteration Incidents in Japan Exploiting BHEK2" (https://sect.iij.ad.jp/d/2013/03/225209.html) (in Japanese) for a detailed explanation of the malware victims were infected with.

Becky!. This demonstrates that the creator of the malware clearly intended to target Japanese users in attacks. This is not the first time that this trend has been seen. However, care must be taken given the potential impact it could have on Japan. We also confirmed that the Pony specimen obtained by IIJ downloaded scareware called Harddisk Antivirus from C&C servers. This malware is fake security software that scares users to commit direct financial theft. However, as with the functionality of BHEK2 mentioned previously, the settings on the C&C server determine what Pony downloads, so it is possible that other malware was used in tandem with it in this series of attacks.

■ Attack Characteristics and Detection of Alterations

■ Website Alteration Techniques

Attackers normally require administrator privileges to install DarkLeech on a website and make it behave as a redirector. For this reason, we believe that attackers somehow gained administrator privileges ahead of time for the websites altered in the latest incident. We have information that many of the altered websites used server management software called Plesk Panel, and it has been suggested that a vulnerability in Plesk Panel may have been exploited*52. Meanwhile, because Plesk Panel was not used with all of the altered websites, we think that other techniques were used to make the alterations in some cases, such as dictionary attacks on SSH or FTP services, or exploitation of known vulnerabilities in a CMS.

■ Anti-analysis Techniques used in DarkLeech

DarkLeech has the following functions for preventing security administrators and researchers from investigating the infection vectors and obtaining specimens, and evading module detection by legitimate server administrators (see Figure 14).

- Prevention of injection to the same client (one week restriction using a connection source IP list and HTTP cookie)
- Prevention of injection to clients that are not attack targets, such as Web crawlers (User-Agent determined)
- Prevention of injection to server administrator sessions (no injection to connections from a local IP address, requests to URLs including the string “Admin,” or connections from remote hosts listed in utmp)
- Prevention of injection when specific processes (tcpdump, rkhunter, chkrootkit) are running

Additionally, while not part of DarkLeech, functions such as the following have been confirmed on the infectors that victims are redirected to. We believe these are also intended to hinder investigation and analysis.

- Downloaded malware is encoded with a random key each time
- Connections from the same source IP address are blocked (HTTP 502 error returned)

■ Detection of DarkLeech

DarkLeech is loaded as an Apache module, so it is possible to confirm its existence by checking the LoadModule line included in Apache configuration files (httpd.conf, etc.). However, because DarkLeech is installed using an arbitrary file name, when you do not already know all the names of the modules intentionally installed, you cannot tell whether the DarkLeech module is present or not using this method. Another potential method for detecting DarkLeech is to search for the configuration files or temporary files it uses. DarkLeech generates a large number of files with names beginning with the string “sess_” under /var/tmp. This is the default path for PHP session files, so when you do not use PHP, or use it and have changed the session file path, these can be treated as traces of DarkLeech.

Additionally, when using PHP with the default session file path, the following files can be used to identify DarkLeech.

*52 JPCERT/CC published “JPCERT/CC Alert 2013-04-08 Alert regarding the usage of old versions of Parallels Plesk Panel” (http://www.jpcert.or.jp/english/at/2013/at130018.html) after confirmation of multiple Web alteration incidents in which malicious Apache modules were installed on servers running old versions of Plesk Panel. Cisco Systems also indicated in “Possible Exploit Vector for DarkLeech Compromises” (http://blogs.cisco.com/security/possible-exploit-vector-for-darkleech-compromises/) that a vulnerability in a webmail component (Horde/IMP package) included in some versions may have been exploited.

- **/var/tmp/sess_d0c94b5412e3494af1e7db042c59afa2**
  A file that encodes and saves iframe tag content.
- **/var/tmp/sess_dbd2e9556e489478954a3 af93b797244**
  A file used for mutual exclusion when connected to a management server.
- **/usr/lib/libbdl. so. 0**
  A file that encodes and saves the host name of the management server (this file is not present in some cases).

Countermeasures

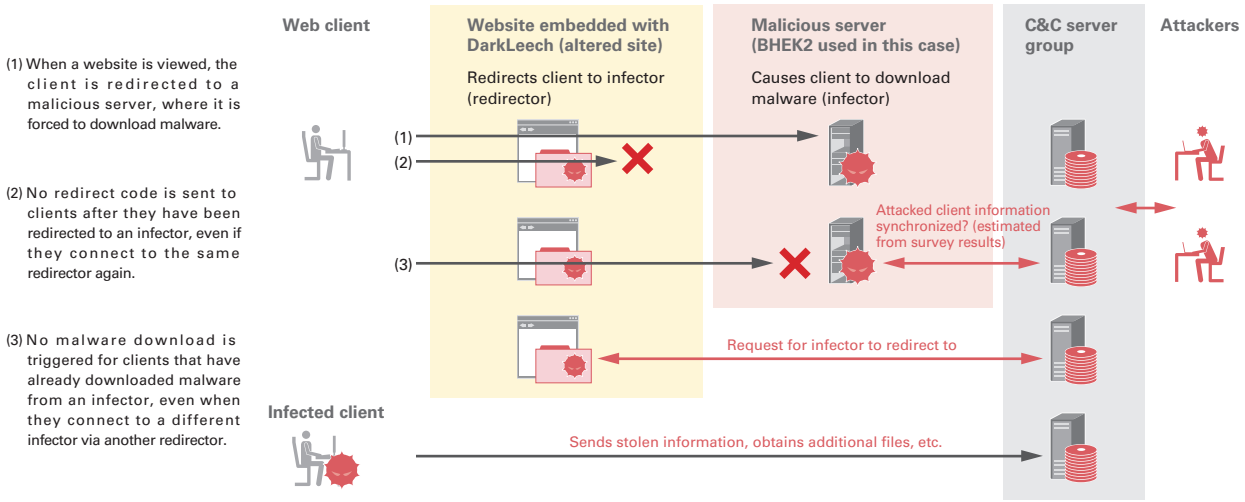
Reports of the existence of DarkLeech began from around August 2012*53. Attacks of this type using BHEK2 in Japan were reported from around January 2013*54, and based on IIJ observations, attacks still continued as of April 2013. Similar attacks are expected to continue in the future, so website operators and PC administrators must implement suitable countermeasures from their respective perspectives.

Measures for Protecting Against Website Alterations

Because a variety of techniques are used in website alterations, a wide range of countermeasures are involved, such as changing server and network configurations, or implementing security diagnostics or security devices. Here, we strongly recommend thoroughly implementing the following three points as a basic countermeasure.

- Keep the applications, plug-ins, and libraries used free of vulnerabilities to protect against attacks exploiting them.
- Set strong passwords, and restrict administrator communication connections and repeated authentication attempts to protect against brute-force attacks.
- Establish a system of obtaining and monitoring logs for public services to identify attack attempts from outside.

Even when using easy-to-use hosting services or cloud services to run a smaller website, we recommend looking at the service specifications and operator skill levels to check that suitable measures are in place.



*Analysis of DarkLeech and malware specimens, as well as the infector behavior observed, indicates that separate C&C servers exist for the redirector, infector, and malware. However, these control components may not all be operated by the same entity. BHEK2 and DarkLeech are also resold in a form similar to SaaS, so a series of attacks may consist of a dynamic combination of components used by different entities.

Figure 14: The Flow of a Series of Drive-By Download Attacks, and Mechanisms for Obstructing Analysis

*53 DarkLeech is cited in articles such as "RFI: Server-wide iframe injections" (http://blog.unmaskparasites.com/2012/08/13/rfi-server-wide-iframe-injections/) and "Malicious, Apache Module Injects Iframes" (http://blog.unmaskparasites.com/2012/09/10/malicious-apache-module-injects-iframes/) on the Unmask Parasites. Blog.

*54 See the Trend Micro security blog posts "Alterations in Japan and Overseas Using Malicious Web Server (Apache) Modules" (http://blog.trendmicro.co.jp/archives/6888) (in Japanese) and "Blackhole Exploit Kit Run Adopts Controversial Java Flaw" (http://blog.trendmicro.com/trendlabs-security-intelligence/blackhole-exploit-kit-run-adopts-controversial-java-flaw/) for more information on the alterations made in this incident, as well as related cases.

Measures to Protect Client PCs from Malware Infection

In user environments, it is important to ensure that the OS and third-party applications are updated, and anti-virus software is installed and kept up to date. Although they involve some operational overheads, implementing vulnerability mitigation tools such as EMET or configuring software restriction policies can also be effective. The Click-to-Play function implemented in Mozilla Firefox and Google Chrome is another effective feature, particularly with regard to attacks targeting browser plug-ins*55. This is disabled in both browsers by default, so to use it the settings must be changed.

1.4.3 Exercises on Responding to Cyber Attacks

In January of this year, the Cyber Attack Exercise Working Group of the Telecom Information Sharing and Analysis Center Japan (Telecom-ISAC Japan) held exercises on responding to cyber attacks. These exercises were quite extensive, being attended by eight major Japanese providers including IIJ, as well as a number of critical infrastructure providers*56. Internet-related exercises have been held around the world in recent years, and their value is recognized. In this report we will give an overview of exercises on responding to cyber attacks, take a detailed look at their planning, and discuss their implementation and effect.

Major Exercises on Responding to Cyber Attacks

Table 1 shows the major Internet-related exercises on responding to cyber attacks. A well-known example is Cyber Storm, which has been held by the United States Department of Homeland Security (DHS) every two years since 2006. Cyber Storm IV took place between fall of 2011 and 2012, and this exercise provided detailed confirmation of whether adequate responses were made over time to incidents that were underway. For the 2012 sessions of Cyber Europe, held every year in the EU, there were 571 attendees from 339 organizations, including 60 ISPs and 60 financial organizations in the EU. In Asia the APCERT Drill is held by APCERT, and APCERT Drill 2013 that took place in January of this year was attended by 22 CSIRT teams from 18 countries. Exercises covering a wide range of sectors are also held in Japan. For example, the Ministry of Internal Affairs and Communications held the "Exercise on Responding to Cyber Attacks in the Telecommunications Industry" over a period of three years from 2006. This involves exercises on defending against attacks on environments simulating critical infrastructure company networks using an actual Internet environment. As these examples demonstrate, cyber attack exercises are conducted in a variety of regions around the world.

Exercise Planning and Implementation

A range of preparations are required when implementing an exercise. Here we give an overview of the basic planning and implementation of an exercise.

Setting Objectives

When planning an exercise, it is first necessary to clarify the objectives of the host and participants, and create a scenario for the exercise that can meet these objectives. For example, if the objective of an exercise is to confirm emergency response procedures within your own organization and identify issues, then you must incorporate events that enable this to be confirmed into the scenario. This means that sufficiently reconciling the objectives of all participants before creating the scenario is a crucial point.

The People Involved in Exercises

The following roles are involved in the planning and implementation of exercises.

- Scenario Planner: Plans exercise scenarios that pull together the objective and events generated by the expected threat
- TA (Trusted Agent): Provides advice regarding the scenario during planning on behalf of the participants
- Director: Presides over the exercise as a whole
- Controller: Passes information on to players during an exercise, and prompts them to decide on a response
- Player: The participants that the exercise revolves around, who respond to events while it is underway
- Evaluator: Sequentially records and evaluates the players' discussions and behavior during an exercise

*55 Click-to-Play is a function that prompts for user confirmation (via a click) instead of executing plug-ins automatically. Because the plug-in display area is often concealed for drive-by downloads, the OK button is also not seen. This means there is no danger of users clicking it accidentally.

*56 Social infrastructure that provides services essential to people's lives and social activities. Currently, 10 critical infrastructure sectors are designated. National Information Security Center (NISC), "An Overview of the Critical Infrastructure Team: Critical Infrastructure Explained" (http://www.nisc.go.jp/active/infra/outline.html) (in Japanese).

More people may be assigned to different roles depending on the exercise content. For example, when a scenario is hard to govern due to multiple events occurring simultaneously, separate controllers and players may be assigned to each event to ensure that there is no impact on the progress of the scenario.

Table 1: Major Internet-Related Exercises

Inaugural Year	Frequency	Country/ Region	Responsible Organization	Exercise Name	Main Organizations Participating	Objective
1996	Annual	United States	DEFCON	DEFCON CTF*57	Teams of employees and students	Research the latest attacks and analysis technology, train and secure information security personnel
2003	-	United States	Department of Homeland Security (DHS)	Livewire*58	Communications, energy, finance, and local government bodies	Verify whether emergency response systems actually function after an attack occurs
2006	Biennial	United States	Department of Homeland Security (DHS)	Cyber Storm*59	Ministries, administrative agencies, foreign governments, private-sector corporations	Measure the performance of the cyber attack countermeasures of participating organizations, including the government
2006	Annual	Asia	APCERT	APCERT Drill*60	CSIRT teams from Asia-Pacific countries	Information sharing and collaboration between participating teams, examination of mechanisms for cooperative handling
2006	Annual (until 2008)	Japan	Ministry of Internal Affairs and Communications	Exercise on Responding to Cyber Attacks in the Telecommunications Industry*61	ISPs, critical infrastructure providers, associated groups and ministries	Examine whether executable attack methods and vulnerabilities in systems exist, the extent of damage caused by attacks, and whether emergency response systems actually function
2006	Annual	Japan	National Information Security Center (NISC)	Critical Infrastructure Incident Response Exercise (CIIREX)*62	The CEPTOAR for each critical infrastructure sector and ministries presiding over critical infrastructure	Verification of the effectiveness of systems for information sharing, contact, and collaboration between public and private entities regarding IT failures at critical infrastructure providers
2006	Annual	Japan	Central Research Institute of Electric Power Industry	Cyber Terrorism Exercise for the Electric Power Sector*63	Power corporations and associated companies	Acquisition of knowledge for the evaluation of incident response systems and information security measures
2009	Annual	Japan	National Information Security Center (NISC)	CEPTOAR Training*64	The CEPTOAR for each critical infrastructure sector and ministries presiding over critical infrastructure	Maintaining and improving systems for information sharing
2009	Annual	Japan	Telecom-ISAC Japan, Japan Data Communications Association	Exercise on Responding to Cyber Attacks	ISPs, critical infrastructure providers, associated groups and ministries	Confirmation of collaboration between providers, development of human resources, recognition of issues
2010	Annual	EU	European Network and Information Security Agency (ENISA)	Cyber Europe*65	ISPs and critical infrastructure providers	Confirmation of the cyber incident response plan for Europe created by member nations
2012	Irregular	Japan	Web Application Security Forum Hardening Project	Hardening*66	Teams made up of students, corporations, and company employees	Technological enlightenment and development of human resources for improving the security of websites, and increased mainstream recognition of these technologies
2012	Annual	Japan	Japan Network Security Association (JNSA) SECCON Executive Committee	SECCON CTF*67	Teams of students and company employees (mainly students)	Discover and develop practically-minded information security personnel, and provide a place for putting technology into practice.
2012	-	Japan	Ministry of Economy, Trade and Industry	CTF Challenge Japan	Teams of employees and students (mainly employees)	Discover and develop practically-minded security personnel in Japan, and examine the CTF competition required for places where technology is put to practice.
2013	-	Japan	Ministry of Economy, Trade and Industry	Electric Power / Gas / Building Sector Cyber Security Exercise*68	Electric power, gas, and building business operators, among others	Improve the response to attacks on control systems

*57 Information on past CTF can be found on the following DEFCON site. "Capture the Flag Archive" (http://www.defcon.org/html/links/dc-ctf.html).

*58 Dartmouth College ISTS "ISTS Bulletin Volume 1, Number 1, Spring 2004" (http://www.ists.dartmouth.edu/docs/ists_v1_1_04.pdf).

*59 See the following United States Department of Homeland Security (DHS) site for more information on Cyber Storm. "Cyber Storm: Securing Cyber Space" (http://www.dhs.gov/cyber-storm-securing-cyber-space).

*60 APCERT, "APCERT EMBARKS ON GLOBAL COORDINATION TO MITIGATE LARGE SCALE DENIAL OF SERVICE ATTACK" (http://www.apcert.org/documents/pdf/APCERTDrill2013PressRelease_AP.pdf).

*61 Videos showing footage of this exercise have been published on the following Ministry of Internal Affairs and Communications website. "Exercise on Responding to Cyber Attacks in the Telecommunications Industry" (http://www.soumu.go.jp/menu_kyotsuu/media/080401_1.html) (in Japanese).

*62 National Information Security Center (NISC), "Summary of Interdisciplinary Exercise for Critical Infrastructure [CIIREX 2012]" (http://www.nisc.go.jp/active/infra/pdf/ciirex2012_2_press.pdf) (in Japanese).

*63 This can be confirmed in Shouichi Matsui's presentation "An Overview of Cyber Terrorism Exercises for the Electric Power Sector" from the poster sessions at the "2007 Central Research Institute of Electric Power Research Results Presentation" for the Central Research Institute of Electric Power (http://criepi.denken.or.jp) (in Japanese).

*64 National Information Security Center (NISC), "CEPTOAR Training Summary" (http://www.nisc.go.jp/conference/seisaku/ciip/dai31/pdf/31siryou04-2.pdf) (in Japanese).

*65 ENISA, "Largest cyber security exercise 'Cyber Europe 2012' report published in 23 languages" (http://www.enisa.europa.eu/media/press-releases/largest-cyber-security-exercise-cyber-europe-report-published-in-23-languages-by-eu-agency-enisa).

*66 WASForum Hardening Project, (http://wasforum.jp/hardening-project/) (in Japanese).

*67 JNSA SECCON (Security Contest) Executive Committee, (http://www.jnsa.org/seccon/) (in Japanese).

*68 Ministry of Economy, Trade and Industry, "Cyber security exercise to be held for the electric power, gas, and building sectors - Japan's first cyber security exercise using simulation systems -" (http://www.meti.go.jp/press/2012/02/20130204002/20130204002.html) (in Japanese).

Types of Exercises

Generally speaking, exercises are broadly categorized into practical and paper types, with the type selected based on the objective of the exercise. Practical exercises are implemented using actual environments, or a simulated environment built based on actual environments, so it is easier to replicate events that occur in real life. However, when using an actual environment it is necessary to take into account the impact on primary operations, and the content that can be confirmed and the costs associated with constructing the environment will change according to the accuracy of the simulated environment.

Paper exercises are conducted based on the assumption of an actual environment or a certain set of circumstances configured for simulation purposes. There is no need to carry out any actions for paper exercises, nor are there any restrictions on the response taken, so it is also possible to portray circumstances that would take an extremely long time, or circumstances with physical limitations. On the other hand, as actual response work is not carried out for paper exercises, a lot of detail must be provided for responses and their results when creating scenarios.

Scenario Planning

Once the objectives are determined, it is time to begin planning a specific scenario. Define the background information, threat, and attacker, and then determine the specific attacks or failures that will occur. Additionally, details such as the relationship between participants, the network configuration, the equipment used, and the application versions are confirmed and added to the scenario as you build it.

The TA (Trusted Agents) selected from participating companies play a crucial role at this stage. TAs act on behalf of the various participants to check whether the scenario created by the scenario planner is any different in terms of the scope of routine work at their companies, comparing areas such as human resources, network environment, and operating procedures. They also provide advice to help facilitate the smooth running of an exercise. The responding department and flow varies depending on the participating service provider. To make an exercise run smoothly, each event must be fine-tuned to match the environment of companies. For paper exercises in particular, because surveys and configuration are not actually carried out, it is necessary to embed the survey results and configuration details, as well as responses taken by your players and their results, into the scenario. This is an arduous task, but it adds more of a sense of realism to the exercise scenario, leading to players responding based on their roles as they would in a regular work environment.

Scenarios are further scrutinized through rehearsals, etc. Ultimately, they are summarized in a detailed list of events called a MSEL (Master Scenario Event List). The MSEL contains all information necessary for running an exercise, such as the times that events will be introduced, the behavior expected from players for each event, and detailed survey results for the circumstances. Directors and controllers use this to conduct the exercise. Scenario planning is very complex and time-consuming, but the refinement of a scenario has an impact on subsequent results, so careful preparation is required.

Implementation of Exercises

Exercises are implemented in a manner similar to that shown in Figure 15. Unlike competitions, exercises are not for vying with other companies, or evaluating and criticizing specific individuals. This fact should be made known to all participants in advance. When it is necessary for players to contact another provider regarding a response to an event introduced by the director, the contact method determined in advance is used to issue a request or query. A tool specially made for the exercise or paper memos are sometimes used to conduct this communication. Players take action regarding the events introduced based on their regular work responsibilities, rather than executing a special response for the exercise. Controllers run the scenario by presenting information to players and answering their questions. Evaluators record the actions taken by players, as well as their reasons for taking them. The scenario is affected in many cases, such as when players do not respond in the expected way. Directors confirm the overall status, make adjustments together with the controllers for each provider, and take the players' actions into consideration while making sure the scenario proceeds smoothly.

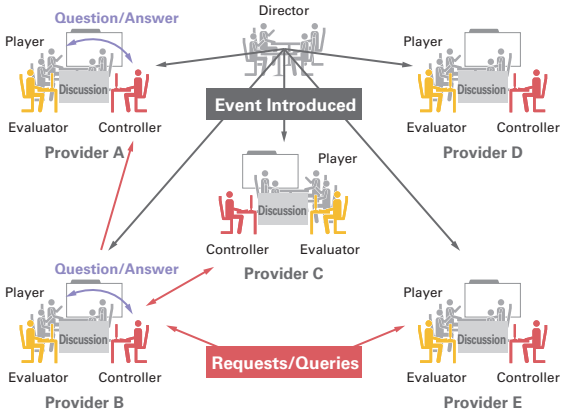


Figure 15: Exercise Overview

Collation of Results and Sampling of the Outcome

After an exercise, results are always collated and the outcome determined. At this point, the entire scenario is revealed to the players, including details of the attacks that occurred during the exercise, as well as the network configuration. First, the overall scenario is confirmed, with controllers working together with players to check what types of threats and events occurred, as well as the objectives of these events. Next, they share the judgment each player made based on the limited information available during the exercise, and the reasons for the actions taken, while checking the records made by evaluators. Also, if there were any misunderstandings between the circumstances occurring in a scenario and the actions taken at the time of response, they confirm and discuss why this happened.

The outcome is ultimately summarized in an After Action Report*69 that collates information from all the organizations participating in an exercise. This outlines the actions of participants, so everyone can share the outcome. The outcome includes items and issues that require remedy, which is valuable information for making improvements to actual practices.

Merits of Exercises

Exercises make it possible to clearly identify issues and points for improvement in the results and outcome summarized in the After Action Report. Many of the events triggered in an exercise would cause serious complications if they actually occurred. Experiencing these circumstances in mock form ahead of time allows organizations and providers to improve their incident handling ability and augment their initiatives. It is also an opportunity for collaboration between providers. Providing participants from different providers or multiple different departments of the same company with experience in orchestrating a concerted response also contributes to the development of personnel with broader perspectives.

Summary

As we have explained here, planning and implementing an exercise requires a great deal of effort. The larger the scale of the exercise, the more complicated and costly the scenario planning becomes. However, although there is a cost involved, some of the experience and knowledge that can be gained through these exercises is hard to find anywhere else. IIJ will continue to actively participate in creating systems for collaboration and cooperative handling between providers through activities such as exercises.

1.5 Conclusion

This report has provided a summary of security incidents to which IIJ has responded. This time was gave an overview of the large-scale incident that occurred in South Korea in March, examined cases of malware infection caused by a large number of alterations that occurred in Japan, and discussed exercises that are attracting attention for improving incident handling ability and cultivating human resources. IIJ makes every effort to inform the public about the dangers of Internet usage by identifying and publicizing incidents and associated responses in reports such as this. IIJ will continue striving to provide 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, Service Operation Division, IIJ. After working in security services development for enterprise customers, Mr. Saito became the representative of the IIJ Group emergency response team, IIJSECT 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, and Information Security Operation providers Group Japan.

Hirohide Tsuchiya, Hiroshi Suzuki, Hisao Nashiwa (1.2 Incident Summary)
Hirohide Tsuchiya, Hiroshi Suzuki, Hisao Nashiwa (1.3 Incident Survey)
Masafumi Negishi, Hiroshi Suzuki, Takahiro Haruyama (1.4.1 The 3.20 Cyber Attack in South Korea)
Hisao Nashiwa, Hiroshi Suzuki (1.4.2 Website Alterations and Drive-By Downloads in Japan)
Hirohide Tsuchiya (1.4.3 Exercises on Responding to Cyber Attacks)
Office of Emergency Response and Clearinghouse for Security Information, Service Operation Division, IIJ

Contributors:
Masahiko Kato, Yuji Suga, Tadashi Kobayashi, Yasunari Momoi, Seigo Saito
Office of Emergency Response and Clearinghouse for Security Information, Service Operation Division, IIJ

*69 The materials from exercises are usually only shared among participants, with little publically available, but the following CYBER STORM III report produced by the United States Department of Homeland Security (DHS) is an example of materials available to anyone. "CYBER STORM III Final Report" (http://www.dhs.gov/sites/default/files/publications/nppd/CyberStorm%20III%20FINAL%20Report.pdf).