Anonymous's OpJapan

In this report we examine the state of Anonymous's operations targeting Japan, and discuss the Flame malware, as well as the ZeuS malware and its variants.

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 April 1 through June 30, 2012. In this period warnings were issued and efforts made to remove the DNS Changer malware, due to the impending shutdown of the DNS server referenced by infected users planned for July. As a result, there were no major disruptions when the server was taken offline on July 9, successfully bringing the incident to an end. However, other malware activities are ongoing. Moreover, it was reported that in the United States a natural gas pipeline serving as critical infrastructure was targeted by cyber attacks, and multiple campaigns targeting Japanese companies and government-related institutions were carried out by Anonymous. A number of server providers in Japan suffered large-scale outages, drawing significant attention to the issue of availability. 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 April 1 and June 30, 2012. Figure 1 shows the distribution of incidents handled during this period*1.

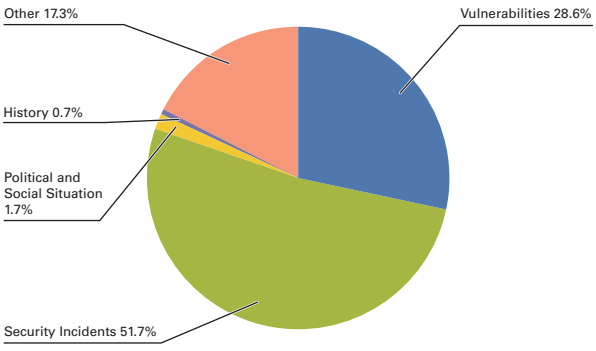

Figure 1: Incident Ratio by Category (April 1 to June 30, 2012)

*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.

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 as well as company sites in a large number of countries stemming from a variety of incidents and causes.

After beginning its activities in late March, Anonymous China become more active in April, and there were alterations or information leaks due to the hacking of several hundred websites for government institutions and local authorities in China. In the U.K., DDoS attacks were made on the website for the Home Office in April in protest against the extradition of a detained suspect to the United States. During the same period, attacks were also made against multiple U.K. government sites, including the Office of the Prime Minister. Additionally, protests against the ACTA treaty*2 become increasingly active in Europe, with government-related sites, related organizations, and companies in European countries targeted in attacks. At the same time DDoS attacks were launched in protest against the CISPA bill in the U.S., targeting organizations such as defense contractors and telecommunications industry groups that had shown support for the bill. Protests against CISPA have continued since then, with information leaks through hacking and DDoS attacks affecting a number of government institutions and companies. A large number of attacks triggered by things such as government regulations also occurred, including DDoS attacks made on multiple government institutions in India in relation to government filtering of the Internet.

Attack campaigns targeting global companies included OpColtan, an offshoot of OpGreenRights that protested against problems associated with the excavation of rare metals in the Democratic Republic of the Congo from late May. This operation targeted a number of companies including mobile phone, semiconductor, and raw material manufacturers, leading to DDoS attacks and information leaks through hacking at multiple companies.

OpNewSon, which also targeted global companies, become a talking point in some circles when several Japanese companies were included in the list of attack targets first published. This operation ended in failure, with no Japanese companies being attacked, and the attack itself not being significantly large. OpJapan was another operation targeting Japan. This campaign began with Anonymous associates that had already been active in Japan conducting demonstrations against ACTA. However, when overseas Anonymous members joined the campaign this escalated into attacks on Japanese government institutions and copyright organizations in protest against the incorporation of criminal punishment for illegal downloading into the amended Copyright Act. These included alterations and DDoS attacks on the websites of a number of government institutions, political parties, and companies. See “1.4.1 Anonymous Attack Campaigns Targeting Japan” for more information about these incidents.

Incidents and Trends at Government Institutions

Attacks other than those by Anonymous on government institutions and related organizations also continued, with the sending of malware, website alterations, and DDoS attacks ongoing. During this period a large number of e-mails misrepresented as being from the Cabinet Office were sent with malware attached. Other incidents include the partial alteration of the website for the National Institute of Information and Communications Technology following unauthorized access, and the discovery of malware infections on terminals used at the Japan Nuclear Energy Safety Organization.

In light of this, and in response to cyber attacks against government ministries, the Cyber Incident Mobile Assistant Team (CYMAT) was established in June, as a government initiative to provide technical support and advice to stop damages from spreading, restore services, investigate causes, and prevent reoccurrence.

From April 21, the automatic distribution of self-signed certificates from GPKI certificate authorities*3 began for Adobe Reader and Adobe Acrobat. Previously it was necessary for users to install these individually. In response, the National Information Security Center published “Countermeasures Against Cyber Attacks Related to the Alteration of PDF Files”. This document details countermeasures against attacks related to the alteration of PDF files, which are a format many

*2 An agreement regarding international responses to infringement of intellectual property rights through the spread of counterfeit goods and pirated copies, etc. See the following page about this topic on the Ministry of Foreign Affairs site for more information. “Anti-Counterfeiting Trade Agreement (ACTA)” (http://www.mofa.go.jp/policy/economy/i_property/acta.html).

*3 The authentication infrastructure used by Japanese government institutions, including the certificate authorities for the certificates required to use digital signatures. See the following page about government authentication infrastructure for more information. “Government Public-Key Infrastructure (GPKI)” (https://www.gpki.go.jp/) (in Japanese).

April Incidents

1 **3rd:** Old Java plug-ins were added to the Mozilla Firefox blocklist, disabling them to reduce security risks.
Mozilla Blog, "Blocklisting Older Versions of Java" (http://blog.mozilla.org/addons/2012/04/02/blocking-java/).

2 **4th:** The Ministry of Internal Affairs and Communications issued administrative guidance to two companies that provide public wireless LAN services, asking that they act to prevent the reoccurrence of incidents in which the secrecy of communications was infringed.

3 **5th:** The Cabinet Office issued a warning after emails misrepresented as being from a Cabinet Office email address spread widely from April 4.
"Regarding Emails Misrepresented as being from the Cabinet Office" (http://www.cao.go.jp/press/20120405notice.html) (in Japanese).

4 **9th:** Anonymous launched DDoS attacks on the websites of defense contractors and industry organizations supporting CISPA.
See accounts such as the following from the United States Telecom Association, which was one of the targets, for more information about these attacks. "US Telecom Website Subject of Denial-of-Service Attack"
(http://www.ustelecom.org/news/press-release/ustelecom-website-subject-denial-service-attack).

5 **10th:** A vulnerability (CVE-2012-1182) in Samba that allowed execution of arbitrary code by sending specially-crafted RPC packets was discovered and fixed.
JVN, "JVNDB-2011-005032: A Vulnerability Allowing Arbitrary Code Execution via the Samba RPC Code Generator"
(http://jvndb.jvn.jp/ja/contents/2011/JVNDB-2011-005032.html) (in Japanese).

6 **10th:** A DDoS attack targeted a number of sites in South Korea, including the website for the Central Election Committee.

7 **11th:** Microsoft published their Security Bulletin Summary for April 2012, and released four critical updates including MS12-027, as well as two important updates.
"Microsoft Security Bulletin Summary for April 2012" (http://technet.microsoft.com/en-us/security/bulletin/ms12-apr).

8 **11th:** A number of vulnerabilities in Adobe Reader and Acrobat that could cause a crash or allow execution of arbitrary code were discovered and fixed.
"APSB12-08 Security updates available for Adobe Reader and Acrobat" (http://www.adobe.com/support/security/bulletins/apsb12-08.html).

9 **11th:** New versions of Python were released, fixing a number of vulnerabilities including the HashDoS vulnerability (CVE-2012-1150).
For example, see the following release notes for Python 3.2.3. "Python 3.2.3" (http://www.python.org/download/releases/3.2.3/).

10 **11th:** There was public outcry after it was discovered that a number of applications on Google Play (the official Google marketplace) were sending the personal information of Japanese users to third parties.
See the explanation on the following Symantec blog for more information about these applications. "'The Movie' Malware Steals Personal Information from Japanese Android Users"
(http://www.symantec.com/connect/blogs/movie-malware-steals-personal-information-japanese-android-users).

11 **11th:** The Ministry of Internal Affairs and Communications published an interim report from the "Working Group regarding the Handling of User Information via Smartphones", which had been evaluating the necessary measures regarding the handling of user information.
"Release of the 'Interim Report for the Working Group regarding the Handling of User Information by Smartphones' by the Research Group for ICT Service Issues from a User's Perspective" (http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000073.html) (in Japanese).

12 **12th:** A number of vulnerabilities caused by Java were fixed in Apple's Java for OS X Lion and Java for Mac OS X 10.6.
"About the security content of Java for OS X 2012-003 and Java for Mac OS X 10.6 Update 8" (http://support.apple.com/kb/HT5247).

13 **13th:** Apple released a Flashback malware removal tool for OS X Lion.
"About the security content of Flashback malware removal tool" (http://support.apple.com/kb/HT5254).

14 **13th:** North Korea went ahead with the satellite launch they had previously announced, but the projectile crashed into the Yellow Sea, causing the launch to fail.

15 **18th:** Oracle released their quarterly scheduled update, fixing a total of 88 vulnerabilities in a number of products.
"Oracle Critical Patch Update Advisory - April 2012" (http://www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html).

16 **19th:** A number of vulnerabilities in OpenSSL including those that allowed arbitrary code execution were discovered and fixed.
"OpenSSL Security Advisory [19 Apr 2012]" (https://www.openssl.org/news/secadv_20120419.txt).

17 **21st:** A number of vulnerabilities in WordPress including those that allowed elevation of privileges and cross-site scripting were fixed.
"WordPress 3.3.2 (and WordPress 3.4 Beta 3)" (http://wordpress.org/news/2012/04/wordpress-3-3-2/).

18 **25th:** In response to threats regarding PDF files, the National Information Security Center announced government initiatives including the detection of alterations relating to the automatic distribution of digital signatures using GPKI.
"Countermeasures Against Cyber Attacks Related to the Alteration of PDF Files" (http://www.nisc.go.jp/press/pdf/pdf_kaizan_press.pdf) (in Japanese).

19 **25th:** VMware announced that part of the source code for VMware ESX between 2003 and 2004 had leaked.
"VMware Security Note" (http://blogs.vmware.com/security/2012/04/vmware-security-note.html).

20 **27th:** A vulnerability in the password reset function of Microsoft's Windows Live Hotmail that made it possible to change the password of arbitrary accounts was discovered and fixed.
The fix was reported in the following Microsoft Security Response Team tweet (https://twitter.com/msftsecresponse/status/195568235654021121).

21 **27th:** The Cyber Intelligence Sharing and Protection Act (CISPA), which provides for the sharing of personal information to prevent criminal behavior on the Internet, was passed in the US House of Representatives.
U.S Government Printing Office (GPO), "H.R. 3523 (RFS) - Cyber Intelligence Sharing and Protection Act"
(http://www.gpo.gov/fdsys/pkg/BILLS-112hr3523rh/pdf/BILLS-112hr3523rh.pdf).

22 **30th:** A Japan-U.S. summit was held, and "Japan-U.S. Cooperative Initiatives" advocating activities such as the construction of a framework for cooperation in cyberspace were announced.
See the following Ministry of Foreign Affairs website for more information. "Prime Minister Yoshihiko Noda's Visit to the United States of America" (http://www.mofa.go.jp/region/n-america/us/pmv1204/index.html).

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

*Dates are in Japan Standard Time

government institutions use when exchanging documents or publishing information. Some of its recommendations include keeping software up-to-date, and checking for alterations using GPKI digital signatures.

In response to the shortage of information security personnel, particularly in the area of dealing with targeted cyber attacks, etc., the National Information Security Center also published "Short-Term Tasks for 2012 and Beyond Based on the Information Security Human Resource Development Program", which summarizes the results of studies by the Information Security Policy Council's "Committee for Public Awareness and Human Resource Development".

■ Vulnerabilities and their Handling

During this period a large number of vulnerabilities were discovered and fixed in Microsoft Windows*4, Internet Explorer*5*6, Word*7, and Office*8*9, and applications such as Adobe Systems' Adobe Reader, Acrobat, and Flash Player, as well as Oracle's Java SE. Fixes were also made to Apple's Java for OS X Lion and Java for Mac OS X 10.6. Several of these vulnerabilities were exploited in the wild before patches were released.

Regarding server applications, a quarterly update for the Oracle database server was released, fixing a number of vulnerabilities. Multiple vulnerabilities in the WordPress CMS including those involving elevation of privileges and cross-site scripting were also fixed. A vulnerability in BIND DNS servers that caused abnormal server stoppages through the use of certain resource codes was fixed. A vulnerability in OpenSSL that made DoS attacks possible by sending specially-crafted data was also fixed.

■ Dealing with the DNS Changer Malware

Regarding the DNS Changer malware*10, the suspension date of the interim DNS server for infected users operated by ISC at the FBI's request was delayed from March 9 to July 9. Because infected users would no longer be able to use the Internet once this DNS server went offline, support was provided for removing the malware and warnings*11 were also sent out.

The Google search engine service and Facebook SNS displayed warning messages when infected users accessed those sites. General warnings were also issued on a large scale, with websites established*12 in countries around the world to enable users to check whether or not they were infected with the DNS Changer malware. In Japan, initiatives such as the publishing of a site for detecting DNS Changer malware infections*13 by the JPCERT Coordination Center, and warnings*14 issued by the Telecom Information Sharing and Analysis Center Japan were carried out.

In part as a result of these efforts, there were no reports of major disruptions in Japan or overseas when the backup DNS server was taken offline at 1:01 PM Japan time on July 9.

*4 "Microsoft Security Bulletin MS12-036 - Critical: Vulnerability in Remote Desktop Could Allow Remote Code Execution (2685939)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-036).

*5 "Microsoft Security Bulletin MS12-023 - Critical: Cumulative Security Update for Internet Explorer (2675157)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-023).

*6 "Microsoft Security Bulletin MS12-037 - Critical: Cumulative Security Update for Internet Explorer (2699988)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-037).

*7 "Microsoft Security Bulletin MS12-029 - Critical: Vulnerability in Microsoft Word Could Allow Remote Code Execution (2680352)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-029).

*8 "Microsoft Security Bulletin MS12-027 - Critical: Vulnerability in Windows Common Controls Could Allow Remote Code Execution (2664258)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-027).

*9 "Microsoft Security Bulletin MS12-034 - Critical: Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight (2681578)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-034).

*10 See "1.4.2 DNS Changer Malware" in IIR Vol.15 (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol15_EN.pdf) for more information about the DNS Changer malware.

*11 JPCERT Coordination Center, "Infections by Malware which Rewrites DNS Settings (DNS Changer)" (https://www.jpcert.or.jp/english/at/2012/at120008.html).

*12 Detection sites for each country can be found on the following DCWG site. "How can you detect if your computer has been violated and infected with DNS Changer?" (http://www.dcwg.org/?page_id=381).

*13 JPCERT Coordination Center, "Announcement of Site for Detecting DNS Changer Malware Infections" (http://www.jpcert.or.jp/pr/2012/pr120002.html) (in Japanese).

*14 Telecom-ISAC Japan, "Warning Regarding DNS Changer Malware Infections" (https://www.telecom-isac.jp/news/news20120530.html) (in Japanese).

May Incidents

1 **S** **1st:** The website for the National Institute of Information and Communications Technology was partially altered after an incident of unauthorized access.
"Unauthorized Access to the National Institute of Information and Communications Technology Website"
(http://www.nict.go.jp/press/2012/05/01-1.html) (in Japanese).

2 **V** **4th:** A number of vulnerabilities in Adobe Flash Player including those that allowed arbitrary code execution by third parties were discovered and fixed.
"APSB12-09: Security update available for Adobe Flash Player" (http://www.adobe.com/support/security/bulletins/apsb12-09.html).

3 **O** **4th:** A planning and operation tie-up between a local authority and a private corporation regarding the use of discount cards at libraries was announced, triggering discussion regarding the handling of personal information such as borrowing history.

4 **O** **7th:** U.S. ICS-CERT issued a warning regarding attacks on a natural gas pipeline.
See the ICS-CERT Monthly Monitor published in May for more information about this incident. "ICS-CERT Monthly Monitor May 2012"
(http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Apr2012.pdf).

5 **V** **9th:** A number of vulnerabilities in Adobe Shockwave Player that allowed arbitrary code execution were discovered and fixed.
"APSB12-13 Security update available for Adobe Shockwave Player" (http://www.adobe.com/support/security/bulletins/apsb12-13.html).

6 **V** **9th:** Microsoft published their Security Bulletin Summary for May 2012, and released three critical updates including MS12-034, as well as four important updates.
"Microsoft Security Bulletin Summary for May 2012" (http://technet.microsoft.com/en-us/security/bulletin/ms12-may).

7 **S** **9th:** DDoS attacks thought to be targeting the channel of a Russian citizen journalist were made on Ustream both in Japan and worldwide.
This incident can be confirmed in tweets from the Ustream (https://twitter.com/ustream/status/200208031617781760).

8 **O** **9th:** Regarding so-called stealth marketing on the Internet, the Consumer Affairs Agency announced they would revise part of the "Issues and Points of Concerns with the Law for Preventing Unjustifiable Extra or Unexpected Benefit and Misleading Representation Regarding Advertisements for Internet Consumer Transactions" due to problems with advertisements not conforming to the Law for Preventing Unjustifiable Extra or Unexpected Benefit and Misleading Representation.
"Regarding Partial Revision of the 'Issues and Points of Concerns with the Law for Preventing Unjustifiable Extra or Unexpected Benefit and Misleading Representation Regarding Advertisements for Internet Consumer Transactions'" (http://www.caa.go.jp/representation/ pdf/120509premiums_1.pdf) (in Japanese).

9 **O** **9th:** The FBI issued a warning via a related organization regarding incidents of malware infections posing as software updates using Hotel Internet connections.
The Internet Crime Complaint Center (IC3), "MALWARE INSTALLED ON TRAVELERS' LAPTOPS THROUGH SOFTWARE UPDATES ON HOTEL INTERNET CONNECTIONS" (https://www.ic3.gov/media/2012/120508.aspx).

10

11 **S** **11th:** Anonymous launched DDoS attacks on multiple Indian government institutions as part of protests (OpIndia) against Internet regulations by the Indian government.

12

13 **V** **15th:** A vulnerability in Apple's QuickTime for Mac OS X that could allow arbitrary code execution via an integer overflow vulnerability was discovered and fixed.
"About the security content of QuickTime 7.7.2" (http://support.apple.com/kb/HT5261).

14 **V** **16th:** It was disclosed that some Logitec wireless LAN broadband router products had a vulnerability that allowed connection IDs and passwords to be obtained externally.
See the following Logitec announcement for more information about this incident. "An Apology and Request Regarding Logitec 300Mbps Wireless LAN Broadband Routers (LAN-W300N/R, LAN-W300N/RS, LAN-W300N/RU2) (http://www.logitec.co.jp/info/2012/0516.html) (in Japanese).

15 **S** **16th:** Anonymous offshoot TheWikiBoat gave advance warning they would launch attacks on May 26 in Operation NewSon, attracting attention due to multiple Japanese companies being targeted.
The details of the first advance warning from April 11 can be found on the site below. PASTEBIN, "Operation NewSon (OpNewSon) #TheWikiBoat" (http://pastebin.com/wq6KdgDg)

16 **O** **17th:** The Ministry of Internal Affairs and Communications held the 18th general meeting of the "Research Group for the Advancement of Internet Usage via IPv6", where issues such as IPv6 fallback in the Japanese Internet environment were discussed.
Ministry of Internal Affairs and Communications, "Research Group for the Advancement of Internet Usage via IPv6"
(http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/ipv6_internet/index.html) (in Japanese).

17

18 **S** **18th:** In relation to the discovery of a number of suspicious Android apps in April, it was reported that the Metropolitan Police Department had searched the premises of IT-related companies in the Tokyo metropolitan area on the suspicion of supplying electromagnetic records of a computer virus.

19 **O** **18th:** The Consumer Affairs Agency presented its viewpoint on item sales techniques in games provided over SNS, indicating it had determined this fell under the category of "card matching", which is prohibited in Item 5 of the Notice of Restricted Prize Goods based on the Law for Preventing Unjustifiable Extra or Unexpected Benefit and Misleading Representation.
"Announcement of our View on "Card Matching" with regard to the Law for Preventing Unjustifiable Extra or Unexpected Benefit and Misleading Representation (Prize Regulations) and Public Comments Regarding the Revision of Guidelines for the Law for Preventing Unjustifiable Extra or Unexpected Benefit and Misleading Representation" (http://www.caa.go.jp/representation/pdf/120518premiums_1.pdf).

20

21 **S** **23rd:** Google began displaying a warning to users suspected of being infected with DNS Changer.
Google Online Security Blog, "Notifying users affected by the DNSChanger malware"
(http://googleonlinesecurity.blogspot.jp/2012/05/notifying-users-affected-by-dnschanger.html).

22

23 **O** **23rd:** The Information-technology Promotion Agency, Japan, published a guide for the implementation of SPF (Sender Policy Framework) as a countermeasure for fraudulent email.
"A Guide to Implementing SPF (Sender Policy Framework) to Eradicate Fraudulent Email" (http://www.ipa.go.jp/security/topics/20120523_spf.html) (in Japanese).

24

25 **S** **26th:** Anonymous offshoot TheWikiBoat went ahead with Operation NewSon, but it ended in failure.

26 **S** **29th:** The sophisticated Flame malware with multiple functions including the eavesdropping of network traffic and the unauthorized transmission of keylogged data was discovered.
See the following Kaspersky Lab SECURELIST Blog post for more information about this malware. "The Flame: Questions and Answers"
(http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers).

27

28

29 **O** **31st:** The Industry Botnet Group (IBG), a private association backed by the United States government, published nine principles for voluntary efforts aimed at reducing the impact of botnets.
"Principles for Voluntary Efforts to Reduce the Impact of Botnets in Cyberspace" (http://www.industrybotnetgroup.org/principles/).

30

31

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

*Dates are in Japan Standard Time

■ Cloud Service Failures in Japan and their Impact

During this period there were failures at a number of hosting service providers. It was discovered that the DNS service provided for one server allowed another party using the same service to register a subdomain of a domain that had already been registered, making it possible for malicious third parties to hijack part of a domain. This issue was later fixed.

At another hosting service provider, problems during maintenance work led to a failure that deleted files, affecting approximately 5,700 customers. It was revealed that most of the data lost in this failure could not be restored, because data backup was not implemented properly. Additionally, because another issue occurred in restored data, it was announced that data would not be restored.

Following these incidents there have been calls to re-examine how cloud and hosting services are used from the perspective of continuity of operations, such as making backups and distributing data and processing between multiple providers.

■ Circumstances Surrounding Smartphones

Work towards the establishment of a public wireless LAN environment is progressing rapidly due to the popularization of smartphones, but along with this trend a range of problems are occurring. It was revealed that providers of a public wireless LAN service at convenience stores were blocking connections to specific e-commerce sites. It also came to light that another public wireless LAN service from a different provider was recording and storing the MAC addresses of user devices as well as account IDs for certain SNS without permission. Both providers have since corrected these issues, but they were subject to administrative guidance from the Ministry of Internal Affairs and Communications due to infringement of the "secrecy of communications" as set forth in Article 4 of the Telecommunications Business Law.

The threat of viruses and malware that target smartphones is also increasing. During this period a number of suspicious apps that targeted Japanese users were discovered among the Android apps published on the official Google Play marketplace, sparking controversy. These apps were given names that made them appear related to popular apps, and when installed they requested excessive permissions, including access to data related to network communications and personal information. When launched they played videos or similar content, but in the background they sent the phone number of the installed device and personal information registered in the address book to an external server. These apps were deleted from the official marketplace once the issues were identified, but it has been pointed out that the personal information of several million users may have leaked. In relation to these incidents, the Metropolitan Police Department conducted searches of the premises of IT-related companies in the Tokyo metropolitan area on the suspicion of supplying electromagnetic records of a computer virus. Apps like these have also been confirmed from sources other than the official marketplace, and the IPA has issued a warning*15.

■ Copyright Act Amendment and Ratification of the Convention on Cybercrime

A bill amending part of the Copyright Act was passed at the Upper House plenary session on June 20. These amendments include the criminalization of DVD ripping and the incorporation of criminal punishment for illegal downloading. The provisions regarding criminal punishment for illegal downloading will come into effect on October 1 this year.

In addition, the Convention on Cybercrime*16 was ratified at a Cabinet meeting on June 26. Although this convention was signed in 2001, its ratification was delayed due to legislation in Japan not being ready. The requirements were met after revisions such as those made the penal code last year*17. With the Instrument of Acceptance deposited to the Council of Europe on July 3*18, the convention is now set to come into effect from November 1 this year.

*15 Information-technology Promotion Agency, Japan, "Warning Regarding Suspicious Apps Targeting Android OS" (http://www.ipa.go.jp/security/topics/alert20120523.html) (in Japanese).

*16 The Ministry of Foreign Affairs has published a Japanese version of this convention. "Convention on Cybercrime (Japan Convention on Cybercrime)" (http://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html) (in Japanese).

*17 See IIR Vol.15 under "1.4.1 Revisions to Unauthorized Computer Access Law" (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol15_EN.pdf) for more information about the development of Internet-related legislation in Japan.

*18 Ministry of Foreign Affairs "On the Deposit of the Instrument of Acceptance of the 'Convention on Cybercrime'" (http://www.mofa.go.jp/announce/announce/2012/7/0704_01.html).

June Incidents

1 **4th:** Microsoft released an update that revoked intermediate CA certificates after confirming that attacks were being made using digital certificates not authorized by a Microsoft Certificate Authority.
"Microsoft Security Advisory (2718704): Unauthorized Digital Certificates Could Allow Spoofing" (http://technet.microsoft.com/en-us/security/advisory/2718704).

2 **5th:** A vulnerability (CVE-2012-1667) in BIND 9 that allowed servers to be terminated was discovered and fixed.
Internet Systems Consortium, "Handling of zero length rdata can cause named to terminate unexpectedly"
(http://www.isc.org/software/bind/advisories/cve-2012-1667).

3 **5th:** Facebook began displaying a warning to users infected with DNS Changer. See the following Facebook Security page for more information.
"Notifying DNSChanger Victims" (https://www.facebook.com/notes/facebooksecurity/notifying-dnschanger-victims/10150833689760766).

4 **6th:** The World IPv6 Launch initiative to activate IPv6 on a permanent basis was implemented, with Web service providers and ISPs from around the world participating.
JAIPA, "Information about the World IPv6 Launch" (http://www.jaipa.or.jp/ipv6launch/index.html) (in Japanese).

5 **6th:** Google began displaying a warning on accounts suspected of being subject to targeted attacks.
Google Online Security Blog, "Security warnings for suspected state-sponsored attacks"
(http://googleonlinesecurity.blogspot.jp/2012/06/security-warnings-for-suspected-state.html)

6 **7th:** A large-scale leak of the SHA-1 password hashes for 6.5 million members occurred at LinkedIn.
See the following LinkedIn Blog for more information about this incident. "An Update on LinkedIn Member Passwords Compromised"
(http://blog.linkedin.com/2012/06/06/linkedin-member-passwords-compromised/).

7 **7th:** JPCERT/CC put out a request for information about the unauthorized use of mail accounts after mail accounts were hijacked at a number of ISPs.
"A Request for Information about Unauthorized Use of Mail Accounts" (http://www.jpcert.or.jp/pr/2012/pr120003.html) (in Japanese).

8 **8th:** In the first application of the revised Unauthorized Computer Access Law, a youth was arrested on suspicion of accessing the server for an online game without authorization and posting user IDs and passwords obtained from it on an Internet message board.

9 **9th:** A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB12-14: Security updates available for Adobe Flash Player" (http://www.adobe.com/support/security/bulletins/apsb12-14.html).

10 **13th:** Microsoft published their Security Bulletin Summary for June 2012, and released three critical updates including MS12-037, as well as four important updates.
"Microsoft Security Bulletin Summary for June 2012" (http://technet.microsoft.com/en-us/security/bulletin/ms12-jun).

11 **13th:** Oracle released a scheduled update for Java SE, fixing a total of 14 vulnerabilities.
"Oracle Java SE Critical Patch Update Advisory - June 2012" (http://www.oracle.com/technetwork/topics/security/javacpujun2012-1515912.html).

12 **13th:** Microsoft published an advisory and temporary FixIT for a vulnerability (CVE-2012-1889) in Internet Explorer that could allow remote arbitrary code execution.
This vulnerability was fixed in the following security bulletin released on July 11. "Microsoft Security Bulletin MS12-043 - Critical: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2722479)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-043).

13 **13th:** A vulnerability in the DNS services of providers that allowed malicious third parties to hijack part of a domain was discovered and fixed.
JPRS subsequently issued a warning about this incident. "Regarding the Risk of Domain Name Hijacking Stemming from Service Operation Issues" (http://jprs.jp/tech/security/2012-06-22-shared-authoritative-dns-server.html) (in Japanese)

14 **19th:** It was reported that attacks had been made exploiting a vulnerability (MS12-037) fixed by Microsoft in June. See the following IBM Tokyo SOC Report for more information.
"Attacks Exploiting an Internet Explorer Vulnerability (MS12-037:CVE-2012-1875) Confirmed"
(https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/ms12-037_20120619?lang=en_us) (in Japanese).

15 **20th:** The bill amending part of the Copyright Act was passed, incorporating criminal punishment for illegal downloading.
Agency for Cultural Affairs, "2012 Regular Diet Session - Regarding Copyright Act Amendments"
(http://www.bunka.go.jp/chosakuken/24_houkaisei.html) (in Japanese).

16 **20th:** A failure occurred in the service of a hosting service provider, leading to the loss of data such as websites and mail for approximately 5,700 customers.

17 **22nd:** It was reported that attacks exploiting an unpatched vulnerability (CVE-2012-1889) in Internet Explorer were occurring.
See the following Symantec Security Response blog for more information. "CVE-2012-1889 in Action"
(http://www.symantec.com/connect/blogs/cve-2012-1889-action).

18 **26th:** Anonymous launched OpJapan, carrying out a number of website alterations and DDoS attacks on Japanese government institutions and related organizations.

19 **28th:** The website of a local public body was targeted in a DoS attack. In relation to this, an incident in which over 10,000 emails were sent via a Web-based mail form also occurred.

20 **29th:** The Ministry of Internal Affairs and Communications published the final report of the "Smart Phone and Cloud Security Research Society".
Ministry of Internal Affairs and Communications, "Final Report of the 'Smart Phone and Cloud Security Research Society' on Recommended Measures for the Safe Use of Smartphones" (http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000020.html) (in Japanese).

21 **29th:** The National Information Security Center announced the establishment of the Cyber Incident Mobile Assistant Team (CYMAT) as a government initiative to provide coordinated mobile support beyond government ministries.
National Information Security Center, "About the Establishment of the Cyber Incident Mobile Assistant Team (CYMAT)"
(http://www.nisc.go.jp/press/pdf/cymat_press.pdf) (in Japanese).

22 **29th:** It was announced that an information leak had occurred when data for a number of customers was mixed up during restoration work after a large-scale failure that took place at a hosting service provider on June 20.

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

*Dates are in Japan Standard Time

The Flame Malware

The Flame malware was discovered in Iran in May. It is thought to have spread mainly in the Middle East region. Full analysis is expected to take several years due to the presence of a large number of modules for each function, and the fact that its size at 20 MB is extremely large for malware.

In addition to spreading via removable disks such as USB flash drives and using a number of known vulnerabilities, a function for spreading the malware to other computers on a local network using fraudulent certificates to launch a MITM attack on the Windows Update mechanism was also confirmed*19. To deal with this problem Microsoft released an update*20 that revoked certificates from intermediate CA thought to be potentially fraudulent. See also "1.4.2 The Flame Malware that Launches MITM Attacks on Windows Update" for more information about this incident.

Usage History and the Handling of Personal Information

During this period the handling of information such as the usage history of IC cards and discount cards used for electronic payments attracted attention.

Discount card numbers were used as part of the authentication process for a wireless LAN service provided at certain convenience stores. However, a number of issues were pointed out, such as the fact that the identification numbers of users' mobile phones were sent inappropriately during this process, and fixes were made. Additionally, when a local public body announced a tie-up with a private corporation to use that corporation's discount card as a library card, it was noted that there would be problems with information such as book borrowing history being used by a private corporation. There were also a number of other incidents where the handling of user information became an issue, such as an incident in which an employee of a railroad company viewed the travel history of an IC card ticket user without authorization.

This type of data that is accumulated on a daily basis is very sensitive, as it can identify individual users, and may even give insight into a user's private life and ideology. This means it requires careful handling.

Other Trends

In other trends, the World IPv6 Launch initiative for promoting the deployment of IPv6 through the permanent activation of IPv6 by ISPs, network device manufacturers, and Web service providers around the world took place. The IPv6-IPv4 fallback issue affecting the FLET'S Hikari service was also discussed at the Ministry of Internal Affairs and Communications' "Research Group for the Advancement of Internet Usage via IPv6". During these discussions Google announced they were creating a list of DNS servers for networks with problems using IPv6*21, and disabling the use of IPv6 from these networks.

Additionally, after incidents in which account information for the user mail services of a number of ISPs were stolen and a large volume of spam sent using these details, the JPCERT Coordination Center called for information on how mail accounts were being obtained. Regarding other incidents in which user mail account information was used fraudulently by third parties, Telecom-ISAC Japan also published a warning due to a sharp rise in such incidents after August 2011*22.

*19 See the following Symantec Official Blog for more information about the function for spreading malware using Windows Update. "W32.Flamer: Microsoft Windows Update Man-in-the-Middle" (http://www.symantec.com/connect/blogs/w32flamer-microsoft-windows-update-man-middle).

*20 "Microsoft Security Advisory (2718704): Unauthorized Digital Certificates Could Allow Spoofing" (http://technet.microsoft.com/en-us/security/advisory/2718704).

*21 The list created by Google can be seen below. "Resolvers to which Google may not return AAAA records." (http://www.google.com/intl/en_ALL/ipv6/statistics/data/no_aaaa.txt).

*22 Telecom-ISAC Japan, "Regarding Spam Sent Using Authentication Information Fraudulently" (https://www.telecom-isac.jp/news/news20111205.html) (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 2 shows the circumstances of DDoS attacks handled by the IIJ DDoS Defense Service between April 1 and June 30, 2012. 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 2 categorizes DDoS attacks into three types: attacks on bandwidth capacity*23, attacks on servers*24, 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 799 DDoS attacks. This averages to 8.8 attacks per day, which is double the average daily number of attacks compared to our prior report. Bandwidth capacity attacks accounted for 0.0% of all incidents, server attacks accounted for 75.9%, and compound attacks accounted for the remaining 24.1%.

The largest attack observed during the period under study was classified as a compound attack, and resulted in 672Mbps of bandwidth using up to 85,000pps packets. Of all attacks, 67.2% ended within 30 minutes of commencement, 24.0% lasted between 30 minutes and 24 hours, and 8.8% lasted over 24 hours. The longest sustained attack was a server attack and compound attack that lasted for four days, one hour, and 22 minutes (97 hours and 22 minutes). During the current survey period attacks of up to 1.97Gbps or 387,000pps were also made on services other than the IIJ DDoS Defense Service.

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*25 and botnet*26 usage as the method for conducting DDoS attacks.

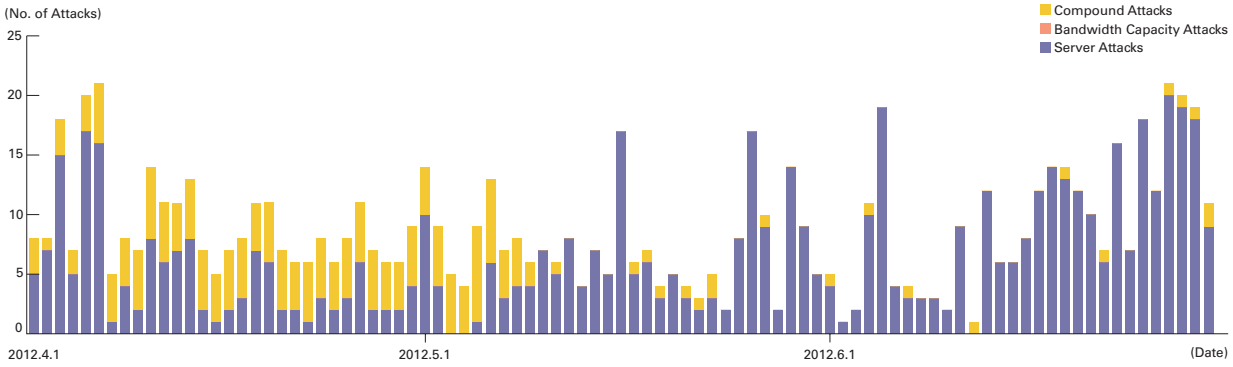

Figure 2: Trends in DDoS Attacks

*23 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.

*24 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.

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

*26 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*27 set up by the MITF, a malware activity observation project operated by IIJ*28. 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 April 1 and June 30, 2012, Figure 3 shows the sender's IP addresses classified by country, and Figure 4 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 59% of the total during the target period. Attacks on ports such as 22/TCP used for SSH, 3389/TCP used for remote desktop, and 443/TCP used for HTTPS were also observed. Looking at the origin of backscatter thought to indicate IP addresses targeted by DDoS attacks by country in Figure 3, the United States and China accounted for large proportions at 37.4% and 22.8%, respectively, with other countries following in order.

Regarding particularly large numbers of backscatter packets observed, there were attacks on the Web servers (80/TCP) for a number of hosting providers in the United States on April 7. Attacks were observed targeting multiple Web servers in China on April 21, the Web server of a file-sharing site in the United States on April 24, and another Web server in China on May 12. A large number of backscatter packets were also observed on May 17, in relation to an attack on a separate hosting provider in the United States.

Many attacks on Web servers (443/TCP) were observed on May 29, May 31, and June 4. These were linked to attacks on the servers of an anti-DDoS service provider in the United Kingdom.

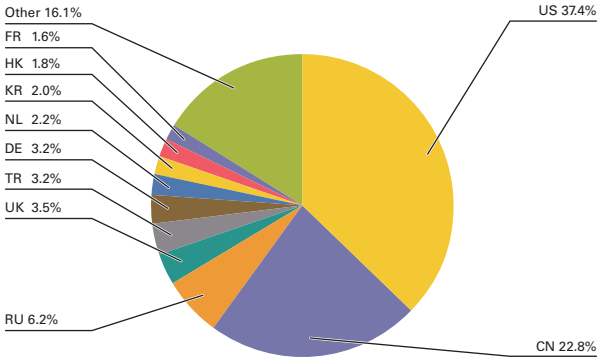

Figure 3: Distribution of DDoS Attack Targets According to Backscatter Observations (by Country, Entire Period under Study)

On April 28 and around April 30 attacks on 20480/TCP targeting servers in the United States were observed. Attacks on 7777/TCP targeting servers in Russia and China were observed between May 13 and May 15. These attacks were made a set number of times on a certain range of IP addresses. Attacks on 7777/TCP targeting servers in Russia were also observed on May 27, but these were made against specific servers. On the same day attacks on 29000/TCP targeting servers in China were also observed. These ports are not normally used by standard applications, so the purpose of the attacks is not known.

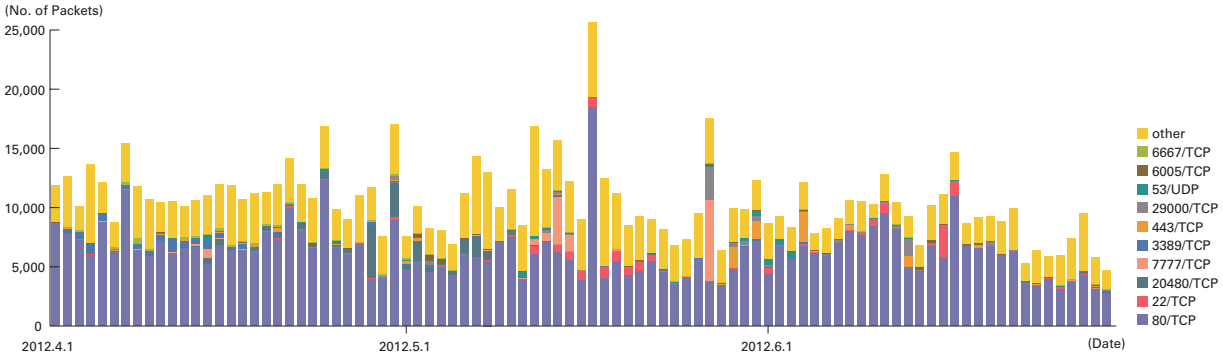

Figure 4: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)

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

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

Notable DDoS attacks during the current survey period that were detected via IIJ's observations of backscatter included attacks by Anonymous on U.K. government sites from April, attacks attributed to UGNazi on U.S. government and local government sites also from April, attacks on a NATO website thought to be the work of Anonymous ATeam in May, and attacks believed to be part of Anonymous's OpColtan in June.

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the MITF*29, a malware activity observation project operated by IIJ. The MITF uses honeypots*30 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 5 shows the distribution of sender's IP addresses by country for communications coming into the honeypots between April 1 and June 30, 2012. Figure 6 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, and 23/TCP used for telnet. Additionally, communications of an unknown purpose were observed on ports not used by common applications, such as 26606/TCP. 54803/UDP communications also rose sharply on May 25, with packets from a large number of sources targeting a specific honeypot intensively for several hours, but the purpose of these communications is not known. 83.4% of the source IP addresses were allocated to Iran. Looking at

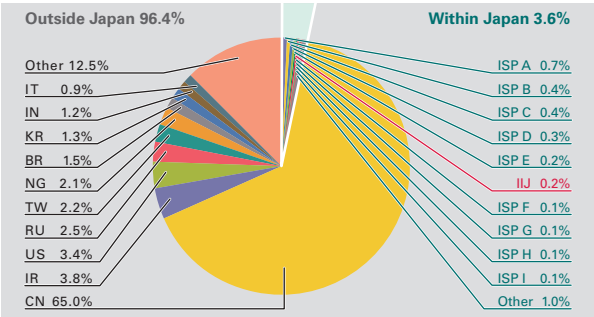

Figure 5: Sender Distribution (by Country, Entire Period under Study)

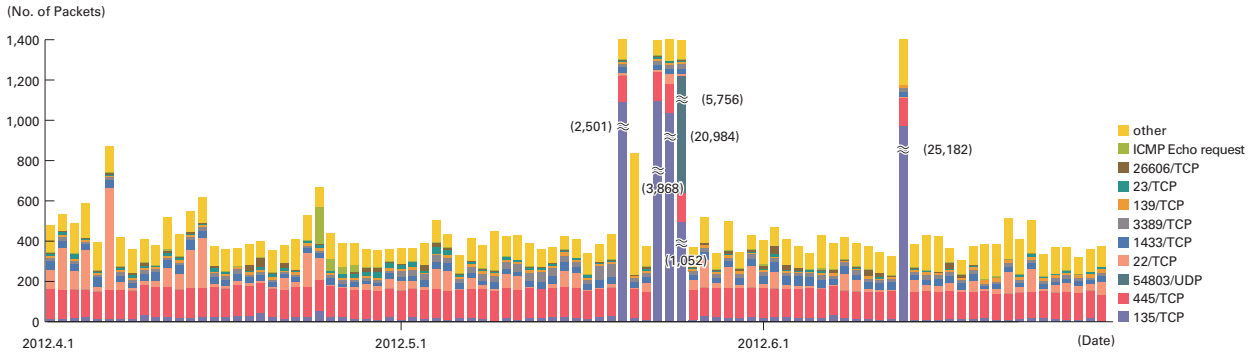

Figure 6: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

*29 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.

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

the overall sender distribution by country in Figure 5, we can see that attacks sourced to China at 65.0%, Iran at 3.8%, and Japan at 3.6% were comparatively higher than the rest.

During the period under study, there were sudden increases in 135/TCP on May 20, between May 23 and May 25, and on June 13. Each of these incidents was caused by large volumes of communications from two IP addresses (that have the same network address) allocated to China. Communications thought to be SSH dictionary attacks also occurred intermittently. For example, concentrated communications were observed coming from individual IP addresses in China, South Korea, and Israel on April 6.

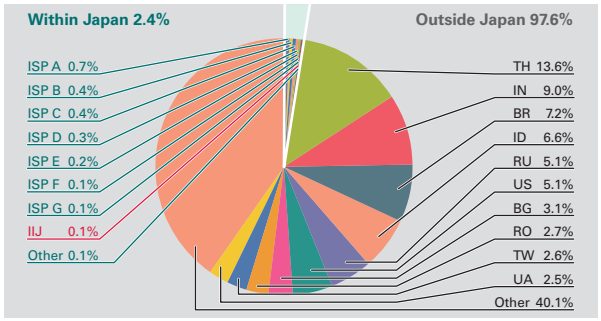

Figure 7: Distribution of Acquired Specimens by Source (by Country, Entire Period under Study, Excluding Conficker)

Malware Network Activity

Figure 7 shows the distribution of the specimen acquisition source for malware during the period under study, while Figure 8 shows trends in the total number of malware specimens acquired. Figure 9 shows trends in the number of unique specimens. In Figure 8 and Figure 9, the number of acquired specimens show the total number of specimens acquired per day*31, while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*32.

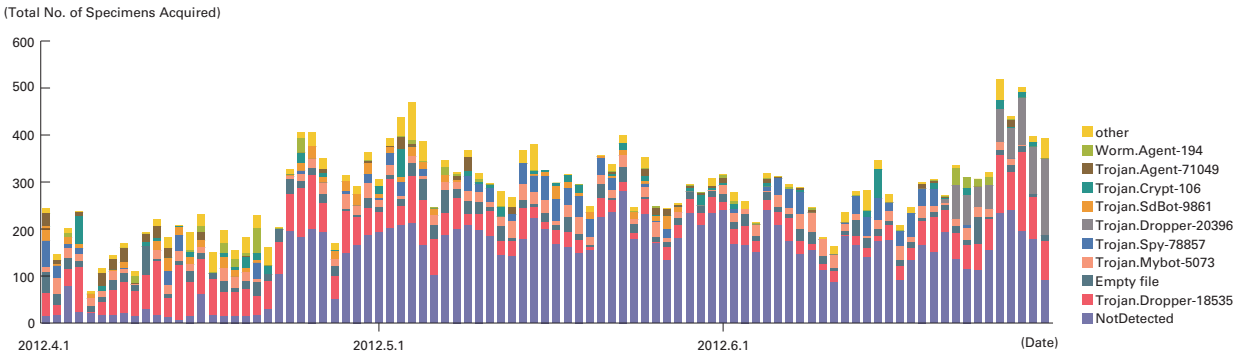

Figure 8: Trends in the Total Number of Malware Specimens Acquired (Excluding Conficker)

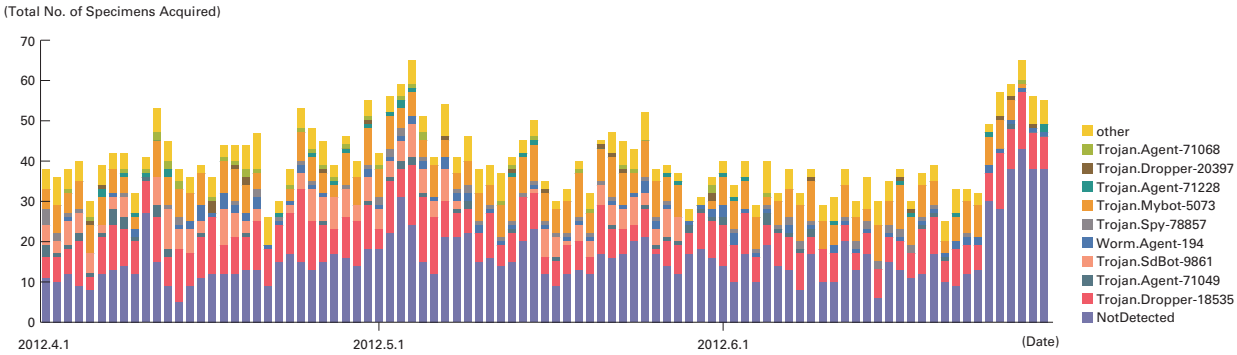

Figure 9: Trends in the Number of Unique Specimens (Excluding Conficker)

*31 This indicates the malware acquired by honeypots.

*32 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.

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 8, and Figure 9 we have detected Conficker using multiple anti-virus software packages and removed any Conficker results when totaling data.

On average, 283 specimens were acquired per day during the period under study, representing 41 different malware. The total number of specimens acquired has doubled since the last report. This is because, after only showing up for part of the previous survey period, unknown specimens from Thailand and Indonesia were in circulation throughout most of the current survey period. After investigating these unknown specimens more closely, we learned that two types of bots*33*34 controlled by IRC servers had been active.

Under the MITF's independent analysis, during the current period under observation 66.3% of malware specimens acquired were worms, 29.9% were bots, and 3.8% were downloaders. In addition, the MITF confirmed the presence of 26 botnet C&C servers*35 and 9 malware distribution sites.

■ Conficker Fluctuations

During this period, changes in the behavior of Conficker were observed. The total number of specimens acquired decreased by about 20% between May 16 and June 19, but subsequently returned to previous levels. It is not known what caused this temporary drop. The survey results show that the drop was not unique to certain specimens, and no regional trends were noted when examining the source IP addresses of specimens acquired.

1.3.3 SQL Injection Attacks

Of the types of different Web server attacks, IIJ conducts ongoing surveys related to SQL injection attacks*36. SQL injection attacks have flared up in frequency numerous times in the past, remaining one of the major topics in the Internet security. SQL injections are known to occur in one of three attack patterns: those that attempt to steal data, those that attempt to overload database servers, and those that attempt to rewrite Web content.

*33 Trojan: Win32/Ircbrute (http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Trojan%3aWin32%2fIrcbrute).
*34 Win32/Hamweq (http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fHamweq).
*35 An abbreviation of "Command & Control." A server that provides commands to a botnet consisting of a large number of bots.
*36 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.

Figure 10 shows the distribution of SQL injection attacks against Web servers detected between April 1 and June 30, 2012. Figure 11 shows trends in the numbers of attacks. These are a summary of attacks detected by signatures on the IIJ Managed IPS Service.

China was the source for 65.4% of attacks observed, while Japan and the United States accounted for 14.5% and 3.1%, respectively, with other countries following in order. Attacks from China increased significantly, because large numbers of attacks were made from China on certain days. Excluding these there was little change from the previous period in the number of SQL injection attacks against Web servers that occurred.

During the current survey period, there were attacks from a specific attack source in China directed at a specific target on June 23. There were also attacks from a separate attack source in China directed at another specific target on June 19. These attacks are thought to have been attempts to find vulnerabilities on a Web server. Attacks occurring on May 10 and June 5 were from a variety of attack sources in Latin American countries, directed at a specific target.

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

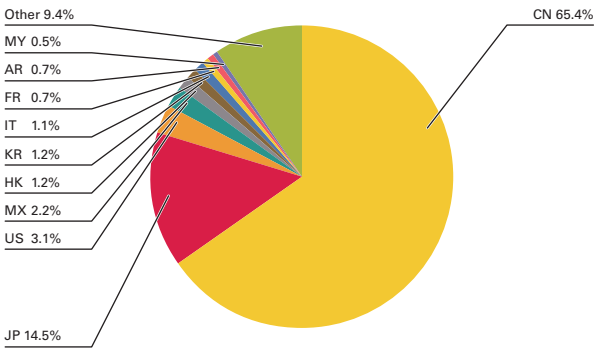

Figure 10: Distribution of SQL Injection Attacks by Source

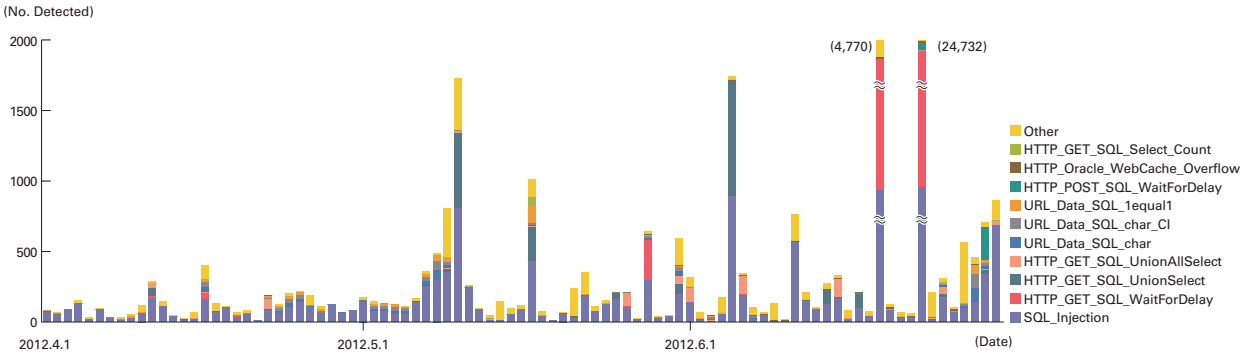

Figure 11: Trends in SQL Injection Attacks (by Day, by Attack Type)

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 present information from the surveys we have undertaken during this period regarding Anonymous attack campaigns in which Japan was targeted, and examine the Flame malware that launches MITM attacks on Windows Update, as well as the ZeuS malware and its variants.

1.4.1 Anonymous Attack Campaigns Targeting Japan

In this report, we look at the circumstances leading up to the Anonymous attack campaigns whose targets include Japan (OpNewSon and OpJapan) that took place between April and June, and provide details about the actual attacks and the responses made to them (Table 1, Table 2).

■ Operation NewSon

On April 11, a group calling themselves TheWikiBoat announced the Operation NewSon (OpNewSon) attack campaign*37. This called for DDoS attacks to be made on May 25 (May 26 Japan time) against 46 major corporate sites, including 3 Japanese corporations. TheWikiBoat is an offshoot of Anonymous consisting of 4 or 5 people, who say they began their activities from April 1. Although they had at one point taken part in Anonymous attack campaigns, they claimed to be independent from Anonymous, and this was virtually the first time they had conducted an attack campaign by themselves. Because the attacks were announced more than a month in advance, the campaign did not draw any attention either in Japan or overseas.

While TheWikiBoat did not make the reasons for the attacks or the basis for selecting targets clear, there was undeniably a possibility that attacks could actually take place. For this reason, as the date announced for the attacks approached, the FBI issued a warning to targeted companies in the United States*38, and similar moves to prepare for the attacks began to be seen in Japan. Reports were also published by some media. Additionally, instructions regarding the attacks started to appear on the IRC channel that TheWikiBoat called on others to join in their announcement.

■ Attack Details

As the start time of the attacks (8AM on May 26 Japan time) approached, more and more participants began joining the IRC channel, which climbed to over 400 users. However, it seems the majority did not take part in the discussion or attacks, and were either there to monitor the activities, or to simply observe passively.

After the start time, TheWikiBoat named an attack target over IRC and Twitter. This target was one of the sites included in the list that was submitted in advance. However, after 30 minutes had passed the site showed no signs of going down, and for some reason the IRC channel was abruptly closed, and the operation discontinued. The attacks were not resumed later, and consequently you could say this operation ended in total failure.

■ Attack Response

Because the attack targets were announced, it was possible for targeted companies to prepare for the attacks in advance. However, looking at the circumstances leading up to the attacks, it is clear that TheWikiBoat was unprepared, meaning a large-scale attack was unlikely. In fact, the responses made to defend against the attacks could be seen as excessive. Some companies were forced to respond without in-depth information, and questions regarding the sharing of information in advance and the ability of organizations to gather and analyze data remain to be answered. It could also be said that a system for responding to emergencies should be in place at all times, instead of responding hastily after advance warning of an attack is given.

Table 1: Operation NewSon

April 1, 2012	TheWikiBoat began its activities.
April 11	TheWikiBoat issued a press release for "Operation NewSon (OpNewSon)". At the same time they published a list of 46 attack targets.
May 23	FOX News was the first major media outlet to report on the attacks.
May 24	The FBI issued an email warning regarding the details of the attack.
May 25	The start time of the attack was announced as 8AM on May 26 Japan time.
May 26	Attacks were made against one site, but they failed.

*37 "Operation NewSon (OpNewSon) #TheWikiBoat" (http://pastebin.com/wq6KdgDg).
*38 Kaspersky Lab Threatpost, "FBI Warns Top Firms Of Anonymous Protest Hacks on May 25" (http://threatpost.com/en_us/blogs/fbi-warns-top-firms-anonymous-protest-hacks-may-25-052412).

Operation Japan

Next, on June 25 Anonymous (AnonOps) issued a press release for Operation Japan (OpJapan)*39. This was done in protest against the amended Copyright Act incorporating criminal punishment for illegal downloading passed by the Diet. Privacy concerns were also voiced regarding an announcement that music rights holders such as JASRAC (Japanese Society for Rights of Authors, Composers and Publishers) were working to have a system for identifying illegal music files*40 implemented by ISPs in Japan. The press release indicated that attacks would be made against the Japanese government and the RIAJ (Recording Industry Association of Japan)*41.

Attack Details

The attacks began with the alteration of a website related to the Ministry of Finance late on the night of June 25. A message from Anonymous left on this site stated that they had launched successful attacks against the Indian government after they tightened Internet regulations (Operation India), and that Japan was their next target.

Full-scale attacks began the following day, on June 26, with a DDoS attack on the website for the Supreme Court, alterations to a website related to the Ministry of Land, Infrastructure, Transport and Tourism, and DDoS attacks on the websites of the Liberal Democratic Party and the Democratic Party of Japan. On June 27 there were also DDoS attacks on the websites for JASRAC and the Japan Business Federation. Although smaller attacks were carried out intermittently after this, as of the time of writing attacks have almost completely subsided. However, given the reasons behind these attacks, the attackers have not achieved their objectives, and it is entirely possible that they could resume at any moment*42.

Attack Response

The targets of these attacks were not made clear in advance, and attacks were launched suddenly against the websites suggested in the IRC channel. Sites thought to have no direct connection to the amendments made to the Copyright Act were also attacked, so it was not a disciplined attack campaign.

Table 2: Operation Japan and Related Events

June 4, 2012	Six rights holders organizations and two companies including JASRAC and RIAJ issued a press release stating their intention to pursue countermeasures against illegal music distribution.
June 9	Anonymous in Japan and other groups joined forces to hold a protest demonstration against ACTA*43 in Sendai.
June 15	Anonymous in Japan announced the "Operation Japan (OpJapan)" protest against ACTA.
June 20	A bill amending part of the Copyright Act (the amended Copyright Act) was passed at the Upper House plenary session.
June 25	Overseas AnonOps issued a press release for "Operation Japan (OpJapan)", which is a protest against the amended Copyright Act, etc.
June 26	A website related to the Ministry of Finance was altered.
	The Supreme Court website was targeted in a DDoS attack.
	A website related to the Ministry of Land, Infrastructure, Transport and Tourism was altered.
	The Liberal Democratic Party website was targeted in a DDoS attack.
	The Democratic Party of Japan website was targeted in a DDoS attack.
June 27	The JASRAC website was targeted in a DDoS attack.
	The Japan Business Federation website was targeted in a DDoS attack.
June 29	The JASRAC website was targeted in a DDoS attack (following this, intermittent small-scale attacks continued).
July 3	Anonymous issued a press release declaring the implementation of Operation Anonymous Cleaning Service/OpA.C.S (promoted by a separate Japanese group of Anonymous that had carried out protests against ACTA).
July 7	The first cleaning meet-up was held in Shibuya, Tokyo.

*39 "#opJapan - Expect US" (http://anonpr.net/opjapan-expect-us-512/).

*40 See the following Copyright Data Clearinghouse site for more information about this system (http://www.cdc.or.jp/).

*41 On June 15 a group calling themselves Anonymous called for protests against ACTA (Anti-Counterfeiting Trade Agreement), and was first to use the name Operation Japan (OpJapan). They also used the same Twitter hashtag, but the groups have no direct connection. The group that conducted a cleanup, or "Operation Anonymous Cleaning Service/OpA.C.S," around the Shibuya station area on July 7 also went by the name Anonymous, but this was carried out by Japanese participants in the wake of the AnonOps attacks. Each of these groups is different, and conducts their activities independently.

*42 Attacks for other Anonymous operations, for example Operation India (OpIndia), have continued for almost a year.

*43 Ministry of Foreign Affairs, "Anti-Counterfeiting Trade Agreement (ACTA)" (http://www.mofa.go.jp/policy/economy/i_property/acta.html).

Although some vulnerable websites were altered, the main method used was DoS attacks. From the IRC channel we believe that tools such as HOIC*44, Slowloris*45, and TorsHammer*46 were used in the attacks. Attacks using a botnet were also observed. Some of the websites attacked became hard to access, indicating a successful DDoS attack, while others appeared unaffected, meaning the attack ended in failure. We believe the results varied based on whether or not a response had been prepared in advance, such as a plan for protecting against DoS attacks, or an emergency system.

■ Future Issues

The OpNewSon and OpJapan attacks were not very large in scale, and as a result their impact was limited. However, they indicate that overseas Anonymous has taken an interest in events in Japan, and with a catalyst this can lead to attack campaigns here. This new development is worth noting, and for the time being it will be necessary to watch for similar activities.

On the other hand, attacks by Anonymous do not require any special countermeasures. As before, it is important to deal with known vulnerabilities to prevent information leaks and alterations to websites, implement DDoS attack countermeasures, and prepare a system for responding to emergencies.

1.4.2 The Flame Malware that Launches MITM Attacks on Windows Update

In this section we give an overview of the malware known as Flame that was discovered in Iran in May 2012, and discuss MITM attacks targeting Windows Update that were made by exploiting this malware to attack the code-signing function.

■ An Overview of Flame

The Flame malware, also known as Flamer or sKyWIper, was discovered by Iran National CERT*47, and has spread mainly throughout the Middle East region. Some reports claim that this malware was developed by the United States and Israel as part of their cyber warfare against Iran. One of the characteristics of Flame is that it has a large number of modules for each function, and the total size of the code for the main components and all modules comes to 20 MB, which is extremely large for malware*48. At the time of writing it has not yet been fully analyzed, but the Laboratory of Cryptography and System Security (CrySyS Lab.) at the Budapest University of Technology and Economics published detailed analysis results*49, and following this security vendors such as Kaspersky Lab each published their own analysis data.

Flame can spread using multiple methods, including via removable devices such as USB flash drives, or by exploiting a number of vulnerabilities*50. One of its most distinguishing features is a function that spreads the malware to other computers on a local network by launching a MITM attack on the Windows Update system*51. Flame also has functions for eavesdropping on communications, collecting account information, capturing screenshots, and recording from microphones. In addition to these, it has a function for analyzing file systems, various documents, and zip archives, and collecting data from them. As this demonstrates, Flame has a host of functions for gathering data from infected terminals and other nearby sources.

*44 HOIC (High Orbit Ion Cannon) is a DoS attack tool that sends a large volume of HTTP GET requests to the target server. It is possible to send a variety of requests by changing the configuration files, which are called boosters.

*45 Slowloris is a DoS attack tool that utilizes vulnerabilities in Web servers such as Apache. It exploits the fact that server processes goes into a standby state when incomplete requests are sent to a Web server.

*46 A DoS attack tool. It resembles Slowloris, but instead of an HTTP GET method, it uses a POST method. It also anonymizes communication routes using Tor (The Onion Router).

*47 Iran National CERT, "Identification of a New Targeted Cyber-Attack" (http://www.certcc.ir/index.php?name=news&file=article&sid=1894).

*48 Kaspersky Lab SECURELIST Blog, "The Flame: Questions and Answers" (http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers).

*49 Laboratory of Cryptography and System Security (Budapest University of Technology and Economics), "sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks v1.05 (May 31, 2012)" (http://www.crysys.hu/skywiper/skywiper.pdf).

*50 In the previously-mentioned report, CrySyS Lab stated that the MS10-061 and MS10-046 vulnerabilities used by Stuxnet may be being used. Kaspersky Lab also stated in the previously-mentioned blog post that the MS10-033 vulnerability may be being used.

*51 A Kaspersky Lab SECURELIST Blog post reported that the Gadget module contained a function for launching a MITM attack by redirecting Windows Update communications to an infected terminal, and installing a code-signed binary on another terminal on a network. "'Gadget' in the middle: Flame malware spreading vector identified" (http://www.securelist.com/en/blog/208193558/Gadget_in_the_middle_Flame_malware_spreading_vector_identified).

■ MITM Attacks on Windows Update

Kaspersky Lab and Microsoft revealed that Flame contained a bypass function that downloads and installs files by disguising them as official program executables signed by Microsoft. Code signing, one of the systems for guaranteeing software reliability, involves digitally signing executables using the PKI framework utilized with SSL/TLS, etc. This makes it possible to eliminate malicious software by verifying the digital signature and issuer when an executable is run*52. Flame is designed to forge this digital signature to make it appear as if Microsoft has signed a file.

When downloading a module via Windows Update, it is possible to guarantee the reliability of software using the code signing function. For example, even if malicious software is downloaded by connecting to a fraudulent server not run by Microsoft via a MITM attack on communications, as long as it is not signed by Microsoft this fraudulent behavior can be detected using the code signing function. However, problems were caused because one of the executables included in Flame is signed using a forged certificate placed in the hierarchy of a PKI certificate trusted by Windows OS, meaning the OS recognizes it as legitimate software. This forged signature originated from defects in the PKI certificate issued by Microsoft that was used, as well as the fact that the already-compromised MD5 was used as the hash function for the digital signature.

After reports of the forged signature, Microsoft released an update on June 3 local time*53. This update revoked three intermediate CA certificates issued by Microsoft that could be used for forgery. The revoked certificates included two different certificates with Microsoft Enforced Licensing Intermediate PCA in the common name (CN) field of the X.509 certificate indicating the subject, and one with Microsoft Enforced Licensing Registration Authority CA (SHA1) in the CN field*54.

Although it is possible to revoke a subset of the certificates by CRL distribution, etc., at this stage the approach of revoking the intermediate CA certificates themselves was taken. Initially, no information was released about how the certificates were forged, and it was thought that Microsoft had overreacted. That said, such measures could be interpreted as being based on the view that a swift response similar to that for the DigiNotar fraudulent issuing incidents would be an effective way of regaining trust.

However, things took a sudden turn in a follow-up from Microsoft published on June 6. It was revealed that MD5 was used as the hash function for the signature of the forged certificate, and the certificate itself had been forged using the chosen prefix collision attack method against MD5*55.

It also came to light that this issue was in part due to the format of the intermediate CA certificates. The certificates contained Key Usage and Extended Key Usage fields that indicate how they are to be used, including information such as Digital Signature, Certificate Sign, CRL Sign, or Code Signing. It was learned that the Microsoft Enforced Licensing Intermediate PCA intermediate CA certificate revoked in this incident including Code Signing, which is beyond the scope of its original intended usage. That means if Code Signing was not included in the usage of the intermediate CA certificate above the forged certificate, it would have been possible to detect the fraudulent usage when the certificate was verified*56.

*52 See the Hardware Dev Center, "Driver Signing Requirements for Windows" (http://msdn.microsoft.com/en-us/library/windows/hardware/gg487317.aspx) for more information about the code signing system.

*53 Microsoft, "Microsoft Security Advisory (2718704): Unauthorized Digital Certificates Could Allow Spoofing" (http://technet.microsoft.com/en-us/security/advisory/2718704).

*54 TechNet Blogs: Security Research & Defense, "Microsoft certification authority signing certificates added to the Untrusted Certificate Store" (http://blogs.technet.com/b/srd/archive/2012/06/03/microsoft-certification-authority-signing-certificates-added-to-the-untrusted-certificate-store.aspx).

*55 TechNet Blogs, "Security Research & Defense, Flame malware collision attack explained" (http://blogs.technet.com/b/srd/archive/2012/06/06/more-information-about-the-digital-certificates-used-to-sign-the-flame-malware.aspx).

*56 For information about similar certificate problems, see IIR Vol.14 under 1.4.1 "Problems Related to the Issuing of Public Key Certificates" (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol14_EN.pdf) regarding issues with the issuing policy at DigiCert Sdn. Bhd.

Figure 12 shows an overview of the behavior of the Flame malware. The certificate associated with WuSetupV.exe, which Flame attempts to install as part of its behavioral sequence, was forged and not signed by Microsoft*57*58. This forged certificate, with the common name "MS", was guaranteed as a real certificate by tracing the certificate path back to the root certificate "Microsoft Root Authority". There have been other successful attempts at forging intermediate CA certificates in the past, but this is thought to be the first time the vulnerability of the MD5 algorithm has posed a threat of this level in the real world.

The Certificate Forgery Technique

The certificate used for the forged signature Flame uses is thought to have been created using cryptographic attack methods against the certificate itself. At one point I believed this forgery used the chosen prefix collision attack*59 disclosed at EUROCRYPT 2007, applying this to a technique for creating forged intermediate CA certificates made public at the end of 2008*60. However, IIJ has confirmed that the format of these forged results and the format of the certificate used by Flame are different. Previous techniques made successful attacks by inserting dummy data into the Netscape Comment extension. However, the forged certificate we obtained does not include the X.509v3 extension, and dummy data has been inserted into the Issuer Unique Identifier instead. This dummy data contains information such as the CRL Distribution Point, reusing the signature part of an existing legitimately-issued certificate to cleverly rewrite the signer just as other previous forgeries.

At the time of writing the method used to create this certificate has not been identified, but the investigation is progressing. First, the researchers who disclosed the previously-mentioned attack technique have uncovered the fact that the certificate was forged using a completely new chosen prefix collision attack*61. Furthermore, a member of that research team has

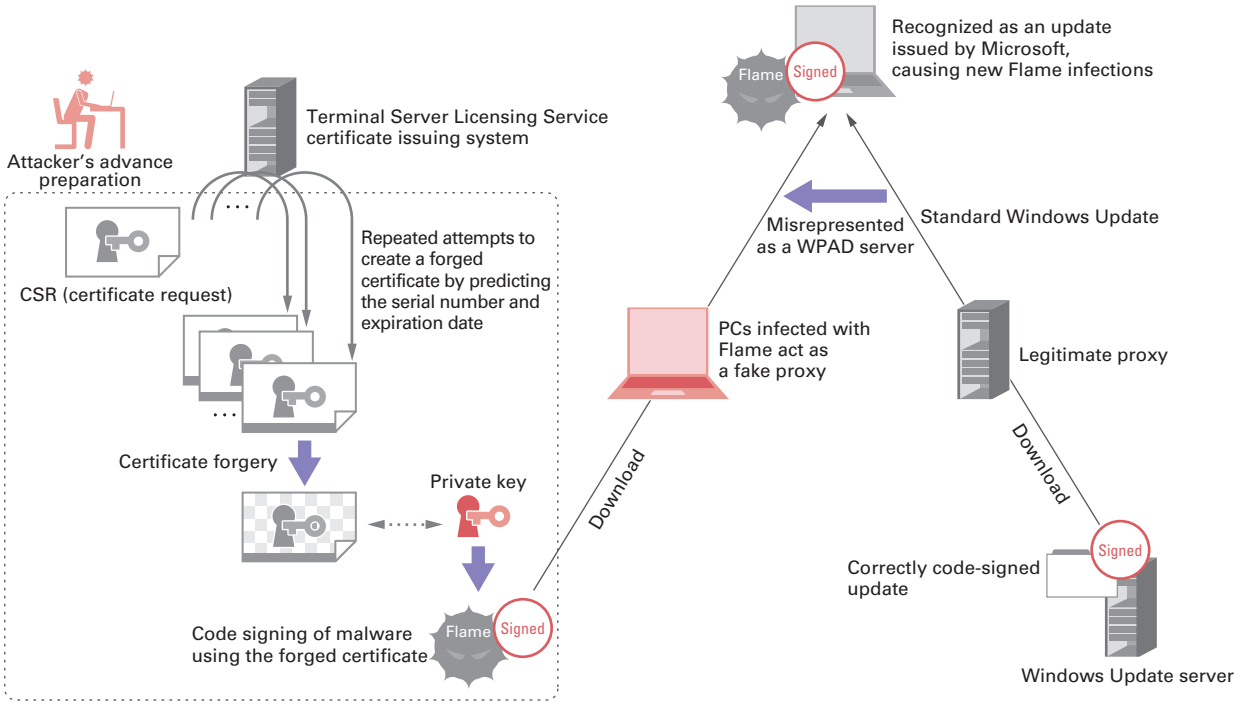

Figure 12: Overview of Flame Malware Behavior

*57 F-Secure Blog, "Microsoft Update and The Nightmare Scenario" (http://www.f-secure.com/weblog/archives/00002377.html).
*58 CrySyS, "The Flame malware WuSetupV.exe certificate chain" (http://blog.crysys.hu/2012/06/the-flame-malware-wusetupv-exe-certificate-chain/).
*59 Marc Stevens, Arjen Lenstra, Benne de Weger, "Chosen-Prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities", EUROCRYPT 2007.
*60 Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, Benne de Weger, "MD5 considered harmful today" 2008 (http://www.win.tue.nl/hashclash/rogue-ca/).
*61 Centrum Wiskunde & Informatica, "CWI cryptanalyst discovers new cryptographic attack variant in Flame spy malware" (http://www.cwi.nl/news/2012/cwi-cryptanalist-discovers-new-cryptographic-attack-variant-in-flame-spy-malware).

published a detailed report regarding the forged certificate*62. Similar to the intermediate CA certificate forgery technique, this report presents a method for obtaining a certificate that causes the attacker's desired signer data to be detected as legitimate by anticipating the serial numbers allocated by the certificate issuing system. However, this attack requires a significant amount of computational power because the serial number stores data accurate to the millisecond that is allocated when a certificate is issued, and it is not known if this technique was used to forge the certificate in this incident.

■ Fundamental Measures Taken by Microsoft

Due to the Flame problem, Microsoft is carrying out a fundamental review of many areas and launching new initiatives. On June 12, an update that automatically processes revoked certificates was released*63. In the past, it was necessary to use Windows Update or manually update information to revoke certificates, but this update made it possible to apply the latest update information for revocation automatically within about a day. In a regular update the following month, an update that revoked 28 certificates was also distributed*64. This was done to prevent potential forgery attacks using forged signatures similar to those carried out by Flame by eliminating problematic certificates. Also, an update that blocks RSA keys less than 1024 bits, which it is recognized should only be used by those understanding the risks involved, is planned for release in August*65*66. Specifically, an error message will be displayed when certificates with RSA keys less than 1024 bits are used for SSL or S/MIME. In order for PKI to be used worry-free, in addition to these initiatives it will be necessary to come up with a system for preventing the use of cryptographic algorithms and key lengths that are known to be dangerous and build an industry-wide consensus, such as blocking certificates using MD5.

1.4.3 ZeuS and its Variants

ZeuS is a crimeware kit*67 that was first discovered around 2007. In March of this year, Microsoft carried out a successful takedown of the majority of ZeuS botnets in conjunction with companies in the financial industry*68. Meanwhile, since the ZeuS source code leaked onto the Internet in May of last year*69, a number of variants thought to be based on ZeuS have been confirmed. These include quite a few variants that could not be detected at all by anti-virus software, and those that contained new functions.

When investigating a computer infected with the ZeuS bot (henceforth ZeuS), you are likely to want to identify the following data.

- The botnet server URL for detecting traces of infections in other computers
- The list of URLs that ZeuS targets for obtaining information, as well as the information actually stolen, to ascertain the damage caused.

*62 Alex Sotirov, "Analyzing the MD5 collision in Flame" (http://trailofbits.files.wordpress.com/2012/06/flame-md5.pdf).

*63 TechNet Blogs, "Announcing the automated updater of untrustworthy certificates and keys" (http://blogs.technet.com/b/pki/archive/2012/06/12/announcing-the-automated-updater-of-untrustworthy-certificates-and-keys.aspx).

*64 Security TechCenter, "Microsoft Security Advisory (2728973): Unauthorized Digital Certificates Could Allow Spoofing" (http://technet.microsoft.com/en-us/security/advisory/2728973).

*65 Windows PKI blog, "RSA keys under 1024 bits are blocked" (http://blogs.technet.com/b/pki/archive/2012/06/12/rsa-keys-under-1024-bits-are-blocked.aspx).

*66 Windows PKI blog, "Blocking RSA Keys less than 1024 bits (part 2)" (http://blogs.technet.com/b/pki/archive/2012/07/13/blocking-rsa-keys-less-than-1024-bits-part-2.aspx).

*67 Crimeware kit refers to a framework for creating malware that steals personal information such as accounts and passwords (particularly those related to finance) from a computer. SpyEye is another crimeware kit. See IIR Vol.13 under "1.4.2 SpyEye" (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol13_EN.pdf) for more information about SpyEye.

*68 See the following blog post for more information about Microsoft's takedown of the ZeuS botnet. "Microsoft and Financial Services Industry Leaders Target Cybercriminal Operations from Zeus Botnets" (http://blogs.technet.com/b/microsoft_blog/archive/2012/03/25/microsoft-and-financial-services-industry-leaders-target-cybercriminal-operations-from-zeus-botnets.aspx).

*69 Around the time that the ZeuS source code leaked, Trend Micro voiced concerns that the leaked source code could be used by criminal organizations. Trend Micro MALWARE BLOG, "ZeuS Source Code Leaked, Now What?" (http://blog.trendmicro.com/the-zeus-source-code-leaked-now-what/).

ZeuS leaves data such as that mentioned above in the registry and file system, and sends and receives it over networks. However, it is unfortunately not easy to confirm the content of the majority of this data. This is because ZeuS implements a sophisticated data encryption scheme, using a number of keys stored in multiple data structures for encryption. To understand this scheme, it is first necessary to grasp how ZeuS handles data.

In this section, we will first look at ZeuS infection behavior with a focus on data handling, based on examination of leaked source code and analysis results for recently-confirmed variants. Next, we will discuss methods for investigating traces of ZeuS infections and encrypted data based on this behavior. Last of all, we will touch upon new functions that have been added to recent variants.

■ ZeuS Bot Infection Behavior

The infection behavior of ZeuS consists of two main parts: the initial installation, and code injection and server communications for stealing information after installation. Figure 13 shows an overview of this infection behavior. ZeuS uses a more complicated data structure than SpyEye. First we will explain its behavior and the main data structures.

Straight after it is run, ZeuS initializes two data structures. These are defined as BASECONFIG and COREDATA. BASECONFIG contains an URL for first accessing the botnet server*70, and an RC4 key based on a constant string. COREDATA contains information such as the OS GUID and version, execution path, and some DLL address, as well as a data structure called PESETTINGS that is only initialized during installation. After initialization of BASECONFIG and COREDATA is complete, if it is the first execution the installation process begins, or otherwise the code injection and server communications processes begin.

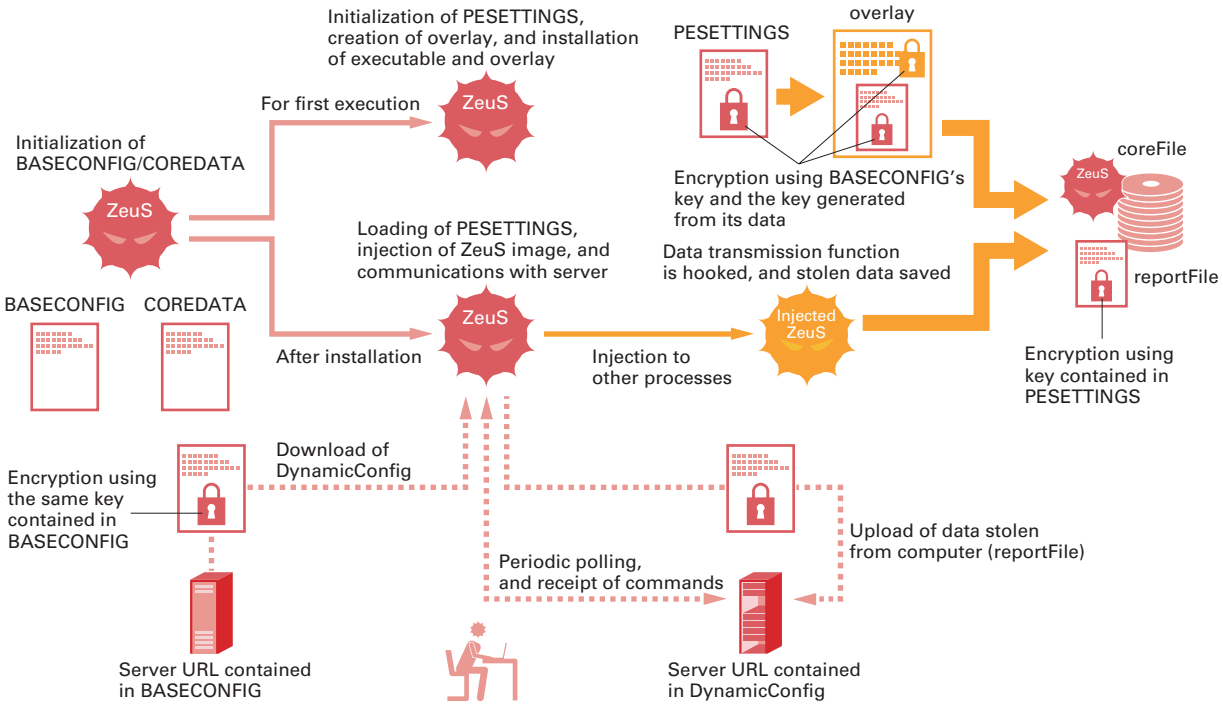

Figure 13: ZeuS Bot Infection Behavior

*70 ZeuS implements obfuscation for important strings using a fixed algorithm. Recent variants use an improved version of the algorithm found in the leaked source code.

Installation

For installation, ZeuS first initializes PESETTINGS. PESETTINGS contains information such as the file system and registry paths (userPaths) used by ZeuS, as well as an RC4 key based on randomly-generated binary data. After PESETTINGS is initialized, it is encrypted using the RC4 key contained in BASECONFIG. The encrypted PESETTINGS is then embedded in data with headers indicating its size, CRC value, and signature*71, after which it is once again encrypted using an RC4 key based on the BASECONFIG data. This data is known as an overlay. When ZeuS copies the executable to the installation folder (coreFile) listed in userPaths, it embeds the overlay into the executable, or saves it as a stand-alone file in the same installation folder*72.

The userPaths value also contains the file path information for saving data that is sent to the server (reportFile), and coreFile and reportFile are both created with random names under the folder specified in CSIDL_APPDATA*73. Finally, installation is completed by creating a process for the installed executable, and deleting an executable of the current process from the file system.

Code Injection and Server Communications

For code injection and server communications, ZeuS first extracts PESETTINGS from the overlay, and checks that the OS GUID and process execution path match those in PESETTINGS. If they match, it catalogs the processes running on the system, and injects the ZeuS executable into any processes that it can. ZeuS hooks the data transmission functions of injected processes, and saves stolen information to the reportFile.

After injection is complete, ZeuS accesses the URL contained in BASECONFIG, and acquires configuration data called DynamicConfig from the server. This data is encrypted, so ZeuS decrypts it using the RC4 key contained in BASECONFIG, and performs a XOR*74 operation to restore it to its pre-encryption state. After confirming details such as the hash value of the data, ZeuS once again performs a XOR*75 operation on the data, and encrypts it using the RC4 key contained in PESETTINGS, before setting the value to the registry. The registry path is determined from the regKey and regDynamicConfig values contained in userPaths, based on "HKCU\SOFTWARE\Microsoft". Subsequently, data is acquired from the registry and decrypted each time DynamicConfig is referenced.

Once DynamicConfig is acquired, ZeuS begins full-scale communications with the botnet server URL (CFGID_URL_SERVER_0) contained within it. Specifically, it conducts polling to confirm its presence, sends information stolen from the computer (data added to the reportFile), and receives and executes commands specified by the server.

Extracting Traces of Infection and Data

By understanding the infection behavior of ZeuS and the data structures it uses that we have detailed above, it is possible to decrypt and parse data left behind on computers infected with ZeuS, as well as data transmitted over a network. This information is useful for detecting traces of infection on other computers and ascertaining damages.

For example, by decrypting the overlay and extracting PESETTINGS using the BASECONFIG data, we can identify the reportFile path and registry values related to configuration such as DynamicConfig*76. Additionally, we can extract DynamicConfig from the registry values through decryption using the RC4 key contained in PESETTINGS and XOR processing.

*71 The 4-byte data "DAVE" is used as the signature.

*72 Depending on the variant, some embed the overlay into the executable, while others save it as a stand-alone file.

*73 For Windows XP this is "C:\Documents and Settings\User Name\Application Data", and for Windows Vista and 7 it is "C:\Users\User Name\AppData\Roaming". See the following article for more information about CSIDL (constant special item ID list). "CSIDL" (http://msdn.microsoft.com/en-us/library/windows/desktop/bb762494%28v=vs.85%29.aspx).

*74 Without using an immediate value, a decremented XOR operation is used on adjacent bytes from the end of the encoded data to the beginning of the data.

*75 Without using an immediate value, an incremented XOR operation is used on adjacent bytes from the beginning of the encoded data to the end of the data.

*76 The timestamps for the installed executables and overlays are changed to avoid forensic investigation, but we have not noted any changes made to the timestamps for the subfolders each is stored in over the course of our analysis to date. As the last modified time of the registry is also unchanged, it is possible to locate relevant data such as the file system and registry path information by conducting a simple timeline investigation.

It is also possible to extract the URL that ZeuS uses to download DynamicConfig from BASECONFIG, and extract the URL of the server that ZeuS regularly communicates with and sends stolen data to from DynamicConfig, which is useful when investigating traces of infection on a network. DynamicConfig also contains a list of target URLs for stealing information (CFGID_HTTP_INJECTS_LIST), meaning you can assume that if a user accessed a URL on the list and input authentication information after they became infected, there is a high chance that this information was stolen. If data transferred over a network was captured, this data can be extracted by decrypting it using the RC4 key contained in BASECONFIG and applying XOR processing.

■ Expansion of Functions in Variants

A number of functions that were not present when the source code was leaked have been added to recently discovered ZeuS variants*77. These functions are executed via commands issued from botnet servers, and include the following.

```
user_activate_imodule
user_restart_imodule
user_start_syn
user_stop_syn
user_start_ssh_scan
```

The user_activate_imodule command downloads and saves a DLL of a fixed name in the coreFile path from the server. It then loads this DLL, and executes the TakeBotGuid function exported by the DLL. It also stores the DLL handle, the address of the exported function (Init/TakeBotGuid/Start), the botnet server URL, and computer identification data in the expanded COREDATA area. After this, it creates a thread and executes the DLL's Init function. The user_restart_imodule command executes the Start exported function of the DLL downloaded using user_activate_imodule.

The user_start_syn command stores its parameters in the expanded COREDATA area, then executes the Syn exported function of the same DLL.

The user_start_ssh_scan command also stores its parameters in the expanded COREDATA area, but executes the start_ssh_checker exported function of a module not used by the other commands.

IIJ has not been able to obtain the DLLs used by the abovementioned commands during the course of its forensic investigations, so their functions are not known. The F-Secure Blog has also discussed the user_activate_imodule and user_restart_imodule commands*78, but as they have not mentioned the other three, it is speculated that creators of the variants are still implementing new functions.

■ Summary

Although ZeuS is a sophisticated crimeware kit, this sophistication means that many variant creators use it without making drastic modifications. As a result, once ZeuS's handling of data is understood, it is possible to make rapid progress in investigating the traces of infection and encrypted data.

*77 Meanwhile, some variants have omitted functions that were previously found in ZeuS (functions for running a Socks server and sending screenshots, etc.).

*78 F-Secure detailed the behavior of the user_activate_imodule and user_restart_imodule commands at the end of last year, and the content they presented matches the results of IIJ analysis. F-Secure Blog, "Suo Anteeksi: Polite Variant of ZeuS" (http://www.f-secure.com/weblog/archives/00002292.html). user_activate_imodule user_restart_imodule user_start_syn user_stop_syn user_start_ssh_scan

Although criminal organizations commonly use ZeuS in combination with existing systems such as exploit kits*79*80, they also appear to be intent on expanding its features actively using the leaked ZeuS source code. In a report regarding large-scale attacks made for financial gain carried out since the beginning of the year*81, McAfee noted that ZeuS and SpyEye variants used in these attacks were equipped with previously unseen functions for automating illegal remittance transactions and avoiding physical two-factor authentication, etc.

It is clear that crimeware kits such as ZeuS will continue to evolve into more and more sophisticated tools for criminal activity, building upon the techniques developed to date. Incident handlers and malware analysts need to deepen their understanding of the malware so they can respond swiftly when new and more powerful variants appear.

1.5 Conclusion

This report has provided a summary of security incidents to which IIJ has responded. In this volume we discussed the status of Anonymous activities targeting Japan, and examined the Flame and ZeuS malware. By publicizing incidents and associated responses in reports such as this, IIJ will continue to inform the public about the dangers of Internet usage, providing the necessary countermeasures to allow the safe and secure use of the Internet.

Authors:
Mamoru Saito
Manager of the Office of Emergency Response and Clearinghouse for Security Information, 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, IIJ-SECT in 2001, participating in FIRST, an international group of CSIRTs. Mr. Saito serves as a steering committee member of several industry groups, including Telecom-ISAC Japan, Nippon CSIRT Association, Information Security Operation providers Group Japan, and others.

Hirohide Tsuchiya (1.2 Incident Summary)
Hirohide Tsuchiya, Hiroshi Suzuki (1.3 Incident Survey)
Masafumi Negishi (1.4.1 Anonymous Attack Campaigns Targeting Japan)
Yuji Suga (1.4.2 The Flame Malware that Launches MITM Attacks on Windows Update)
Takahiro Haruyama (1.4.3 ZeuS and its Variants)
Office of Emergency Response and Clearinghouse for Security Information, Service Operation Division, IIJ

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

*79 Exploit kits are also detailed in IIJ Technical WEEK 2010 “Security Trends for 2010 (1) Web Infection Malware Trends” (http://www.iij.ad.jp/company/development/tech/techweek/pdf/techweek_1119_1-3_hiroshi-suzuki.pdf) (in Japanese).

*80 For example, Kaspersky Lab examined a case in which the BlackHole exploit kit was used to install ZeuS after exploiting vulnerabilities. SECURELIST Blog, “A gift from ZeuS for passengers of US Airways” (http://www.securelist.com/en/blog/208193439/A_gift_from_ZeuS_for_passengers_of_US_Airways/).

*81 In their analysis report, McAfee looked at case studies related to this attack, and examined points where it had evolved beyond previous crimeware kits. “Dissecting Operation High Roller” (http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf).