Targeted Attacks and Their Handling

In this report we discuss the targeted attacks that have received significant attention since last September, and examine the exploitation of fraudulently issued certificates.

1.1 Introduction

This report summarizes incidents to which IIJ responded, based on general information obtained by IIJ itself related to the stable operation of the Internet, information from observations of incidents, information acquired through our services, and information obtained from companies and organizations with which IIJ has cooperative relationships. This volume covers the period of time from October 1 through December 31, 2011. In this period a number of hacktivism-based attacks by Anonymous and other groups followed in the wake of those from the last survey period, and a series of attacks targeting companies and government-related organizations were discovered. It was also revealed that the hacking of critical infrastructure such as a water delivery system in the United States had occurred. Additionally, with the growing number of smartphone users there has been an increase in the number of issues regarding the handling of user information. As seen above, the Internet continues to experience many security-related incidents.

1.2 Incident Summary

Here, we discuss the IIJ handling and response to incidents that occurred between October 1 and December 31, 2011. Figure 1 shows the distribution of incidents handled during this period[*1].

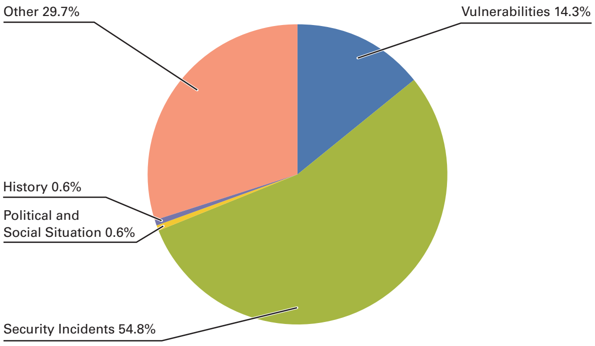


Figure 1: Incident Ratio by Category (October 1 to December 31, 2011)

[*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.

■ Activities of Anonymous, etc.

Attacks by hacktivists such as Anonymous continued during this period. DDoS attacks and information leaks occurred at government-related sites in the United States, Israel, Italy, Portugal, Colombia, El Salvador and many other countries stemming from a variety of incidents and causes. In the United States in particular there were large-scale information leaks from a number of government-related organizations as well as companies.

In September, the Occupy Wall Street protests calling for correction of the widening gap between the rich and the poor began on Wall Street in New York. It gained wide support, and from October demonstrations spread beyond the United States to countries all over the world. Anonymous also indicated their support for these protests by leaking the personal information of executives at major financial institutions and calling for money to be moved from these institutions.

In November they also voiced their opposition to the SOPA (Stop Online Piracy Act) bill that was under deliberation in the U.S. Congress, and threatened attacks on companies that supported SOPA as well as the U.S. government. Deliberation of the bill was postponed as a result of a variety of campaigns opposing SOPA, but at the time of writing attacks by Anonymous are ongoing, and careful attention must be paid to future trends.

In an attack on Stratfor (Strategic Forecasting Inc.) in December, a Web server was hacked, and a list on the server including the credit card information of customers who were subscribed to a report was leaked. Some of this information was released online. There were also financial damages due to incidents using this list such as donations being made to a charitable organization*[2].

■ Targeted Attacks and Their Countermeasures

In Japan, it was discovered that targeted attacks detected by a major corporation in September had also been made against other leading companies and a number of government institutions. During this period a series of targeted attacks against multiple government-related organizations were identified. In one case there were reports of damages including the leaking of user IDs and passwords as well as email content. The Cabinet Secretariat issued an alert in December*[3] because of the repeated attacks on government institutions.

Due to this series of targeted attacks many countermeasures have been implemented, with government institutions taking the lead. First, the chief cabinet secretary released a message*[4] about reinforcing information security measures in relation to this issue, and government initiatives were also discussed by the Information Security Policy Council*[5]. A number of countermeasure activities have also been implemented by various ministries and agencies*[6]. Systems for helping general companies by tracking information and supporting countermeasures are being put together, including warnings about targeted attack emails from the JPCERT coordination center*[7], and the establishment of a “special consultation service for targeted cyber attacks” by the IPA*[8], to name a few*[9]. See “1.4.2 Targeted Attacks and Their Handling” for more information.

*2 Details of this incident can be found in the following F-Secure blog post. “About Anonymous, Donations and Charities” (http://www.f-secure.com/weblog/archives/00002288.html).

*3 National Information Security Center (NISC), “Managing Administrator Privileges Appropriately as a Countermeasure for Targeted Attacks” (http://www.nisc.go.jp/press/pdf/hyoutekigata_press.pdf) (in Japanese).

*4 The message released by the chief cabinet secretary who serves as head of the Information Security Policy Council can be seen on the site for the office of the Prime Minister below. “Reinforcing Information Security Measures” (http://www.kantei.go.jp/jp/tyokan/noda/20111007message.html) (in Japanese).

*5 Information Security Policy Council (http://www.nisc.go.jp/conference/seisaku/index.html) (in Japanese).

*6 For example, “Police Initiatives Regarding Cyber Intelligence Measures” (http://www.npa.go.jp/keibi/biki3/230804kouhou.pdf) (in Japanese) by the National Police Agency, the “Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP)” (http://www.ipa.go.jp/security/J-CSIP/index.html) (in Japanese) by the Ministry of Economy, Trade and Industry, or the “Telecom-ISAC Public-Private Council” by the Ministry of Internal Affairs and Communications. Private-sector businesses such as security operation providers and critical infrastructure companies have also been looking into similar measures.

*7 JPCERT Coordination Center, “JPCERT/CC Alert 28.10.11 Targeted Email Attacks” (http://www.jpcert.or.jp/english/at/2011/at110028.txt).

*8 IPA, “‘Special consultation service for targeted cyber attacks’ established” (http://www.ipa.go.jp/about/press/20111025.html) (in Japanese).

*9 Other private sector activities include those by the CEPTOAR Council made up of critical infrastructure companies in Japan, and the Information Security Operation provider Group Japan’s (http://www.jnsa.org/isog-j/e/index.html) Targeted Attack Countermeasure Evaluation Working Group.

October Incidents

S **1st:** An SDK provided to developers of Android apps in Japan became an issue when it was discovered that it acquired data on phones inappropriately.

V **2nd:** A vulnerability making it possible for arbitrary apps to read personal information was discovered in TCLoggers, which is installed on some HTC Android smartphones. A patch for this vulnerability was provided on October 7 in Japan.
Android Police, "Massive Security Vulnerability In HTC Android Devices (EVO 3D, 4G, Thunderbolt, Others) Exposes Phone Numbers, GPS, SMS, Emails Addresses, Much More" (http://www.androidpolice.com/2011/10/01/massive-security-vulnerability-in-htc-android-devices-evo-3d-4g-thunderbolt-others-exposes-phone-numbers-gps-sms-emails-addresses-much-more/).

O **3rd:** The IPA published their report on "Analysis of Targeted Attack Email."
"IPA Technical Watch: Report on 'Analysis of Targeted Attack Email'" (http://www.ipa.go.jp/about/technicalwatch/20111003.html) (in Japanese).

V **5th:** A vulnerability (CVE-2011-3368) that exposed internal servers was patched in the behavior of certain reverse proxy configurations using mod_proxy on Apache.
"Apache HTTP Server: mod_proxy reverse proxy exposure (CVE-2011-3368)" (https://bugzilla.redhat.com/show_bug.cgi?id=769844).

O **5th:** The results of a study on the commercial botnet Aldi Bot were published.
The Arbor Networks Security Blog, "DDoS Watch: Keeping an Eye on Aldi Bot (http://ddos.arbornetworks.com/2011/10/ddos-aldi-bot/).

S **7th:** The Japanese government's Information Security Policy Council decided to give training on targeted suspicious email to approximately 50,000 personnel at government institutions.
National Information Security Center, "27th Assembly Reference Data 1 - Training on Targeted Suspicious Email at Goverment Institutions" (http://www.nisc.go.jp/conference/seisaku/dai27/pdf/27shiryous1.pdf) (in Japanese).

O **7th:** Attacks taking advantage of the news of Steve Jobs' death on the 6th were confirmed.
TrendLabs MALWARE BLOG, "Cybercriminals Remember Steve Jobs Through Facebook Scam" (http://blog.trendmicro.com/cybercriminals-remember-steve-jobs-through-Facebook-scam/).

S **11th:** A major service outage affecting RIM's BlackBerry devices prevented connection to the Internet and the sending or receiving of messages. This issue continued for 3 days in various parts of the world.
"BlackBerry Service Update" (http://www.rim.com/newsroom/service-update.shtml).

O **11th:** A DDoS attack was made on the New York Stock Exchange at the behest of Anonymous.
IIJ-SECT Security Diary, "Anonymous Launches DDoS Attack on NYSE" (https://sect.iij.ad.jp/d/2011/10/127533.html) (in Japanese).

V **12th:** A number of vulnerabilities in Apple's iOS 5 software that could lead to the execution of arbitrary code or information leaks were patched.
"About the security content of iOS 5 Software Update" (http://support.apple.com/kb/HT4999).

V **12th:** A number of vulnerabilities in Apple's OS X Lion that could lead to the execution of arbitrary code or information leaks were patched.
"About the security content of OS X Lion v10.7.2 and Security Update 2011-006" (http://support.apple.com/kb/HT5002).

V **12th:** Microsoft published their Security Bulletin Summary for October 2011, and released two critical and six important updates.
"Microsoft Security Bulletin Summary for October 2011" (http://technet.microsoft.com/en-us/security/bulletin/ms11-oct).

S **14th:** The Duqu malware that featured similar code to Stuxnet and attempted to obtain information via remote access was discovered.
Symantec Security Response Blog, "W32.Duqu: The Precursor to the Next Stuxnet" (http://www.symantec.com/connect/http%3A/%252Fwww.symantec.com/connect/blogs/w32_duqu_precursor_next_stuxnet).

V **18th:** A vulnerability (CVE-2011-3544) in Oracle's Java SE JDK and JRE that allowed the execution of arbitrary code was patched.
"Oracle Java SE Critical Patch Update Advisory - October 2011" (http://www.oracle.com/technetwork/topics/security/javacpuoct2011-443431.html).

O **18th:** The United States Department of Homeland Security was revealed to have issued an alert of the threat of cyber attacks on industrial control systems (ICS) by Anonymous.
public intelligence, "(U//FOUO) DHS Bulletin: Anonymous Hacktivist Threat to Industrial Control Systems (ICS)" (http://publicintelligence.net/ufouo-dhs-bulletin-anonymous-hacktivist-threat-to-industrial-control-systems-ics/).

S **22nd:** An alert was issued about the spread of a worm targeting the "JBoss" open source application server. The vulnerability exploited by the worm was patched in April 2010.
SANS ISC Diary, "JBoss Worm" (http://isc.sans.edu/diary.html?storyid=11860).

S **25th:** The Hacker's Choice released a tool for launching DoS attacks on vulnerable HTTPS sites using SSL renegotiation.
SANS ISC Diary, "The Theoretical 'SSL Renegotiation' Issue gets a Whole Lot More Real!" (http://isc.sans.edu/diary/11893).

S **25th:** Malware that used official Android application updates to infect devices was discovered.
F-Secure Blog, "DroidKungFu Utilizes an Update Attack" (http://www.f-secure.com/weblog/archives/00002259.html).

S **25th:** It was reported that targeted attacks on government-related organizations in Japan had taken place in July.

S **26th:** In South Korea DDoS attacks were launched on websites of the electoral council and candidates for the Seoul mayoral election.

V **28th:** A vulnerability in the WordPress WPtouch plug-in that made SQL injections possible was discovered and fixed.
EXPLOIT-DB, "WordPress wptouch plugin SQL Injection Vulnerability" (http://www.exploit-db.com/exploits/18039).

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

*Dates are in Japan Standard Time

■ Vulnerabilities and their Handling

During this period a large number of vulnerabilities were discovered and fixed in Microsoft Windows*[10] clients and applications such as Adobe Systems' Adobe Reader and Acrobat*[11], Flash Player*[12], and Shockwave Player*[13], as well as Oracle's JRE*[14]. Several of these vulnerabilities were exploited before patches were released. Vulnerabilities were also found in server applications such as the ISC BIND*[15] DNS Server and the Apache HTTPD Server*[16] Web server. Other vulnerabilities were patched in Microsoft Windows*[17] and the ProFTPD*[18] FTP server. A German hacker group also released a proof-of-concept DoS tool targeting an issue with Web server SSL renegotiation*[19]. Additionally, at the 28th Chaos Communication Congress held in Germany, a technique for launching DoS attacks against a large number of Web application development platforms including PHP was disclosed*[20].

■ Alteration of Web Content Exploiting Vulnerabilities

There were also many incidents of hacking-related alterations. There was an increase in attacks targeting vulnerabilities that had been revealed in certain systems, such as a worm*[21] that spread by exploiting a known vulnerability (CVE-2010-0738) in the JBoss Web application server, the TimThumb and ASP.net*[22] plug-ins for the WordPress CMS, the Plone CMS and phpThumb.php*[23]. It was revealed that the Blackhole Toolkit exploit kit had incorporated exploitation of the vulnerability in TimThumb*[24].

Web server applications such as these have become widely used because they are easy to deploy and feature rich functions, but many incidents using automated attack techniques to target vulnerabilities like those mentioned above have been confirmed. Swift steps must be taken to set appropriate access privileges and implement security updates for servers that are exposed to the Internet.

*10 "Microsoft Security Bulletin MS11-087 - Critical: Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2639417)" (http://technet.microsoft.com/en-us/security/bulletin/ms11-087).

*11 "APSB11-30: Security updates available for Adobe Reader 9.x and Acrobat 9.x for Windows" (http://www.adobe.com/support/security/bulletins/apsb11-30.html). Fixes for Adobe Reader X and Adobe Acrobat X were also made available on January 10, 2012: "Security updates available for Adobe Reader and Acrobat" (http://www.adobe.com/support/security/bulletins/apsb12-01.html).

*12 "APSB11-28: Security update available for Adobe Flash Player" (http://www.adobe.com/support/security/bulletins/apsb11-28.html).

*13 "APSB11-27: Security update available for Adobe Shockwave Player" (http://www.adobe.com/support/security/bulletins/apsb11-27.html).

*14 "Oracle Java SE Critical Patch Update Advisory - October 2011" (http://www.oracle.com/technetwork/topics/security/javacpuoct2011-443431.html).

*15 Internet Systems Consortium, "BIND 9 Resolver crashes after logging an error in query.c" (http://www.isc.org/software/bind/advisories/cve-2011-tbd).

*16 Red Hat Bugzilla, "Bug 740045 (- CVE-2011-3368) CVE-2011-3368 httpd:reverse web proxy vulnerability" (https://bugzilla.redhat.com/show_bug.cgi?id=740045).

*17 "Microsoft Security Bulletin MS11-083 - Critical: Vulnerability in TCP/IP Could Allow Remote Code Execution (2588516)" (http://technet.microsoft.com/en-us/security/bulletin/ms11-083).

*18 "Response pool use-after-free memory corruption error" (http://bugs.proftpd.org/show_bug.cgi?id=3711).

*19 See the following SANS ISC Diary for more information about this tool. "The Theoretical 'SSL Renegotiation' Issue gets a Whole Lot More Real!" (http://isc.sans.edu/diary.html?storyid=11893).

*20 See the following presentation for more information about this technique. "Effective Denial of Service attacks against Web application platforms" (http://events.ccc.de/congress/2011/Fahrplan/events/4680.en.html). After this presentation fixes were made to the products involved, but at the time of writing only some of them have been released.

*21 Details of this worm can be found on the following JBoss Community blog. "Statement Regarding Security Threat to JBoss Application Server" (https://community.jboss.org/blogs/mjc/2011/10/20/statement-regarding-security-threat-to-jboss-application-server).

*22 Details of the incident targeting ASP.NET can be found on the following Armorize Malware Blog. "http//jjghui.com/urchin.js mass infection ongoing" (http://blog.armorize.com/2011/10/httpjjghuicomurchinjs-mass-infection.html).

*23 IBM Tokyo SOC Report, "An Increase in Attacks on Plone CMS and phpThumb" (https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/plone_phpthumb_attack_20111226?lang=ja_jp) (in Japanese).

*24 See the following AVAST! Blog for more details. "Following WordPress into a Blackhole" (https://blog.avast.com/2011/10/31/following-wordpress-into-ablackhole/).

November Incidents

S **1st:** A large number of attacks that altered pages using a WordPress vulnerability and infected visitors with malware were confirmed.
Avast! Blog, "Following WordPress into a Blackhole" (https://blog.avast.com/2011/10/31/following-wordpress-into-a-blackhole/).

S **2nd:** It was reported that Japanese government-related organizations other than those mentioned in October have also been hit by targeted attacks around the same time.

S **4th:** It was discovered that a Malaysian SSL certificate authority had issued SSL certificates with low cryptographic strength.
Entrust, Inc., "Entrust Bulletin on Certificates Issued with Weak 512-bit RSA Keys by Digicert Malaysia"
(http://www.entrust.net/advisories/malaysia.htm).

S **5th:** A DDoS tool was discovered on the server of a Dutch SSL certificate authority, and the issuing of certificates was temporarily suspended to investigate.
Kaspersky Lab SECURELIST Blog, "Dutch CA suspends issuance of digital certificates"
(http://www.securelist.com/en/blog/208193210/Dutch_CA_suspends_issuance_of_digital_certificates).

S **7th:** A large-scale DNS cache poisoning incident occurred in Brazil.
Kaspersky Lab SECURELIST Blog, "Massive DNS poisoning attacks in Brazil"
(http://www.securelist.com/en/blog/208193214/Massive_DNS_poisoning_attacks_in_Brazil)

V **8th:** Multiple widespread network outages occurred around the world due to a vulnerability in Juniper routers.
These outages were reported in the following NANOG mailing list thread
(http://mailman.nanog.org/pipermail/nanog/2011-November/041653.html).

V **8th:** Multiple vulnerabilities in Adobe Shockwave Player that made remote execution of code possible were discovered and fixed.
"APSB11-27: Security update available for Adobe Shockwave Player" (http://www.adobe.com/support/security/bulletins/apsb11-27.html).

S **8th:** There was a pump failure at a water facility in Illinois. This incident was initially reported to have been caused by a cyber attack originating from Russia, but it was later announced that no attack had taken place.
ICS-CERT, "ICSB-11-327-01 - ILLINOIS WATER PUMP FAILURE REPORT" (http://www.us-cert.gov/control_systems/pdf/ICSB-11-327-01.pdf).

V **9th:** A vulnerability in the ProFTPD FTP server (CVE-2011-4130) that made remote execution of code possible was discovered and fixed.
bugs.proftpd.org, "Response pool use-after-free memory corruption error" (http://bugs.proftpd.org/show_bug.cgi?id=3711).

V **9th:** Microsoft published their November 2011 security bulletin, and released fixes for the MS11-083 critical update, two important updates, and one warning update.
"Microsoft Security Bulletin Summary for November 2011" (http://technet.microsoft.com/en-us/security/bulletin/ms11-nov).

S **9th:** A DDoS attack was made on a company that provides services to local authorities, affecting 200 local authorities in Japan that use these services.

V **10th:** Multiple vulnerabilities in Adobe Flash Player including those that made remote execution of code possible were discovered and fixed.
"APSB11-28: Security update available for Adobe Flash Player" (http://www.adobe.com/support/security/bulletins/apsb11-28.html).

O **10th:** The Internet Content Safety Association (ICSA) announced the status of the blocking of child pornography to news outlets.
Internet Content Safety Association (ICSA) (http://www.netsafety.or.jp/) (in Japanese).

V **11th:** Microsoft released an update that revoked certificates issued by two intermediate certificate authorities as a measure against weak SSL certificates issued by DigiCert Sdn. Bhd.
"Microsoft Security Advisory (2641690) Fraudulent Digital Certificates Could Allow Spoofing"
(http://technet.microsoft.com/en-us/security/advisory/2641690).

S **14th:** Malware signed using the signing key of an organization related to the Malaysian government was discovered.
F-Secure Blog, "Malware Signed With a Governmental Signing Key" (http://www.f-secure.com/weblog/archives/00002269.html).

S **15th:** It was reported that there had been an increase in the number of website alteration attacks using a vulnerability in a WordPress plug-in that was discovered in August 2011.
IBM Tokyo SOC Report, "An Increase in Alteration Attacks on Websites using WordPress"
(https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/wordpress_injection_20111115?lang=ja) (in Japanese).

V **16th:** A vulnerability in BIND 9 (CVE-2011-4313) that made it possible to bring down servers remotely was discovered and fixed.
ISC, "BIND 9 Resolver crashes after logging an error in query.c" (http://www.isc.org/software/bind/advisories/cve-2011-tbd).

S **19th:** An individual calling themselves pr0f claimed to have hacked into a water facility system (SCADA) in Texas, and released screenshots of several control screens as proof.
Kaspersky Lab Threatpost, "Hacker Says Texas Town Used Three Character Password To Secure Internet Facing SCADA System"
(http://threatpost.com/en_us/blogs/hacker-says-texas-town-used-three-character-password-secure-internet-facing-scada-system-11201)。

O **25th:** The IPA released the "icat" cyber security alert service for distributing the alerts they publish in real-time.
"'icat' Cyber Security Alert Service Released" (http://www.ipa.go.jp/security/vuln/icat.html) (in Japanese).

S **28th:** Researchers announced that the Carrier IQ application installed to smartphones by mobile phone companies had been collecting and sending data on smartphone usage.

O **30th:** The IPA published the "Design and Operational Guide to Cope with 'Advanced Persistent Threats' - 2nd Edition."
"Design and Operational Guide to Cope with 'Advanced Persistent Threats'" (http://www.ipa.go.jp/security/vuln/newattack.html) (in Japanese).

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

*Dates are in Japan Standard Time

■ Attacks on Critical Infrastructure

During this period there were a number of attacks on critical infrastructure. The SCADA system at a water facility in Texas was hacked, and images of control screens released as proof*[25]. Server groups containing electronic application systems for a number of local authorities in Japan were also attacked, affecting application work. Before the incident in Texas an attack on an Illinois water delivery system originating from Russia was reported, but it was later announced that this had been a misunderstanding.

■ The Hacking of Certificate Issuing Authorities and Acquisition of Fraudulent Certificates

Incidents of the hacking of certificate issuing authorities and subsequent issuing of fraudulent certificates continued to occur. A DDoS tool was discovered during the course of a police investigation into a DDoS attack at KPN in the Netherlands, and as a result the issuing of certificates was temporarily suspended to investigate*[26]. A hacking incident using phpMyAdmin also occurred at Gemnet, a subsidiary of KPN that provided security consulting and authentication technology to local authorities and police in the Netherlands*[27]. It is thought that the hacked database contained network information related to these customers. See "1.4.1 Problems Related to the Issuing of Public Key Certificates" for more information about these incidents.

After it was revealed that 22 certificates with low cryptographic strength and no revocation information were issued by Malaysian certificate issuing authority DigiCert Sdn., Microsoft, Mozilla, and others revoked trust in its intermediate authorities*[28].

A final report was also released summarizing the results of an investigation into GMO GlobalSign, which is thought to have been hacked in a series of incidents perpetrated by ComodoHacker. The report indicated that fraudulent certificates had not been issued, and certificate authority infrastructure had not been breached.

■ DDoS Attacks

In South Korea DDoS attacks were launched on the websites of candidates and the electoral council during the Seoul mayoral election held in October, causing disruptions such as preventing information on the location of voting stations from being accessed. Individuals including the secretary of a ruling party Diet member and the president of an IT company were arrested on suspicion of carrying out these attacks*[29]. DDoS attacks related to an election also occurred in Russia, with attacks being made on the websites of radio stations and independent electoral monitoring groups, rendering them inaccessible.

■ Phishing Trends in Japan

During this period phishing incidents utilizing email and SNS continued to occur. In particular, there were similar phishing attacks misrepresenting a number of banks, leading to financial damages in some cases. Attack patterns included use of programs attached to emails, and redirection to a phishing site*[30]. In both cases screens were displayed prompting input of secondary authentication information, etc.

In addition to IDs and passwords for financial institutions, there were also phishing incidents that targeted SNS and online game accounts, leading to damages such as the unauthorized use of points.

*25 Details about the incident can be found in the following Kaspersky Lab Threatpost. "Hacker Says Texas Town Used Three Character Password To Secure Internet Facing SCADA System" (http://threatpost.com/en_us/blogs/hacker-says-texas-town-used-three-character-password-secure-internet-facing-scada-system11201).

*26 Below is the official announcement from KPN. "KPN stopt uit voorzorg uitgifte nieuwe veiligheidscertificaten" (http://www.kpn.com/corporate/overkpn/Newsroom/nieuwsbericht/KPN-stopt-uit-voorzorg-uitgifte-nieuwe-veiligheidscertificaten.htm) (in Dutch).

*27 Details of this incident can be found in the following Sophos Naked Security blog post. "Second Dutch security firm hacked, unsecured phpMyAdmin implicated" (http://nakedsecurity.sophos.com/2011/12/08/second-dutch-security-firm-hacked-unsecured-phpmyadmin-implicated/).

*28 Microsoft and Mozilla's responses were as follows. Microsoft "Untrusted Certificate Store to be updated" (http://blogs.technet.com/b/msrc/archive/2011/11/03/untrusted-certificate-store-to-be-updated.aspx). Mozilla Security Blog, "Revoking Trust in DigiCert Sdn. Bhd Intermediate Certificate Authority" (http://blog.mozilla.com/security/2011/11/03/revoking-trust-in-digicert-sdn-bhd-intermediate-certificate-authority/).

*29 Sophos, Naked Security "Election-day cyber attack scandal rocks South Korea's ruling party" (http://nakedsecurity.sophos.com/2011/12/08/election-cyber-attack-scandal-south-korea/).

*30 These phishing incidents are also explained in the following IPA report. "Computer Virus/Unauthorized Computer Access Incident Report - September 2011 -" (http://www.ipa.go.jp/security/english/virus/press/201109/documents/summary1109.pdf).

December Incidents

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

S **1st:** It was discovered that the .us domain registrar about.us had been altered since September through a vulnerability in WordPress.

S **4th:** In South Korea the secretary for a ruling party Diet member and others were arrested on suspicion of making DDoS attacks on an electoral council website on October 26, 2011.

S **4th:** DDoS attacks were launched on multiple radio stations and opposition party news sites on the day of lower house elections in Russia.
Harvard University, Internet & Democracy Blog "Coordinated DDoS Attack During Russian Duma Elections"
(http://blogs.law.harvard.edu/idblog/2011/12/08/coordinated-ddos-attack-during-russian-duma-elections/).

S **7th:** In the Congo DNS cache poisoning incidents were observed on major websites such as Google.

V **7th:** Vulnerabilities with no fix available were discovered in Adobe Reader and Acrobat.
"APSA11-04: Security Advisory for Adobe Reader and Acrobat" (http://www.adobe.com/support/security/advisories/apsa11-04.html).

S **9th:** A database was hacked at a certificate authority, a subsidiary of Dutch KPN, due to inappropriate settings.
Sophos, Naked Security "Second Dutch security firm hacked, unsecured phpMyAdmin implicated"
(http://nakedsecurity.sophos.com/2011/12/08/second-dutch-security-firm-hacked-unsecured-phpmyadmin-implicated/).

V **13th:** Oracle released Java SE 6u30.
"Update Release Notes JavaTM SE 6 Update 30" (http://www.oracle.com/technetwork/java/javase/6u30-relnotes-1394870.html).

V **14th:** Microsoft published their Security Bulletin Summary for December 2011, and released three critical and ten important updates.
"Microsoft Security Bulletin Summary for December 2011" (http://technet.microsoft.com/en-us/security/bulletin/ms11-dec).

S **14th:** GMO GlobalSign published their final report on the unauthorized access by Comodohacker that came to light in September 2011.
"Security Incident Report" (http://www.globalsign.co.uk/company/press/121411-security-incident-report.html).

O **15th: The National Police Agency released information about the status of Internet banking phishing incidents and violations of the anti-unauthorized access law.**
"Status of Violations of the Anti-Unauthorized Access Law related to Internet Banking" (http://www.npa.go.jp/cyber/warning/h23/111215_1.pdf) (in Japanese).

V **16th:** Known vulnerabilities in Adobe Reader 9 and Acrobat 9 were fixed.
"APSB11-30: Security updates available for Adobe Reader and Acrobat 9.x for Windows"
(http://www.adobe.com/support/security/bulletins/apsb11-30.html).

V **20th:** A denial of service vulnerability in the Unbound DNS cache server was discovered and fixed.
"Unbound denial of service vulnerabilities from nonstandard redirection and denial of existence [VU#209659 CVE-2011-4528]"
(http://www.unbound.net/downloads/CVE-2011-4528.txt).

S **20th:** Targeted attacks taking advantage of news of the death of the Supreme Leader of North Korea were confirmed.
IBM IBM Tokyo SOC Report, "Targeted Attacks Taking Advantage of North Korea Supreme Leader's Death Confirmed"
(https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/targeted_attack_20111220?lang=ja_jp) (in Japanese).

O **22nd:** The National Information Security Center issued an alert about targeted attacks on servers that manage network users.
National Information Security Center, "Managing Administrator Privileges Appropriately as a Countermeasure for Targeted Attacks"
(http://www.nisc.go.jp/press/pdf/hyoutekigata_press.pdf) (in Japanese).

O **23rd:** U.S. Domain registrar the Go Daddy Group withdrew its support for SOPA after a protest campaign was launched against them.
"Go Daddy No Longer Supports SOPA" (http://www.godaddy.com/newscenter/release-view.aspx?news_item_id=378).

S **26th:** Anonymous attacked a major U.S. think tank, leaking personal information that was stored on its servers.

V **29th:** Efficient techniques for launching DoS attacks on many Web application development platforms such as PHP were presented at a security event held in Germany.
28C3, "Efficient Denial of Service Attacks on Web Application Platforms"
(http://events.ccc.de/congress/2011/Fahrplan/attachments/2007_28C3_Effective_DoS_on_web_application_platforms.pdf).

S **29th:** Anonymous announced they would resume attacks on Sony (OpSony) in relation to SOPA.

V **30th:** Microsoft released an update for vulnerabilities that were discovered in the .NET Framework, including those that allowed arbitrary code to be executed.
"Microsoft Security Bulletin MS11-100 - Critical: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2638420)"
(http://technet.microsoft.com/en-us/security/bulletin/ms11-100).

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

*Dates are in Japan Standard Time

■ Duqu Malware

It was discovered that the structure of the malware named Duqu bore a close resemblance to Stuxnet*[31]. Stuxnet was a malware discovered in 2010 that infected certain industrial control systems, and it attracted attention due to the uniqueness of its targets and its complicated structure. The newly discovered Duqu malware does not target industrial systems, but instead attempts to steal information on infected PCs. Later analysis revealed that a number of stolen digital signatures were used in the incorporated driver files*[32], and that a vulnerability in the Windows kernel that was not fixed at the time of discovery was used to spread infections*[33].

■ DNS Cache Poisoning

A large-scale DNS cache poisoning occurred in Brazil, leading to attempts to install a Trojan to steal bank IDs and passwords*[34]. The DNS cache poisoning of major websites in the Congo was also observed. DNS is a system that is essential for use of the Internet, and when DNS cache poisoning is successful serious problems such as redirection to malicious sites or the eavesdropping or alteration of Web or email content can occur.

■ Smartphone App Issues and the Rise of Malware

Together with the increased penetration of smartphones multiple instances of malware targeting these devices have also been discovered. Malware targeting money or the information inside smartphones are on the rise. Overseas, in particular, a large number of malware exploiting Premium SMS*[35] for Android have surfaced, with some even being distributed as official apps through the Android Market*[36].

Issues with the handling of user information by standard apps have also increased. It was revealed that a tool called CarrierIQ for obtaining device information and aggregating it on the mobile phone carrier side was preinstalled in a number of smartphones, causing issues due to various information being sent without the user's knowledge*[37]. The SDKs used to create apps also become a topic of discussion due to them requesting more access privileges than necessary, or in some cases sending user information to an external party without the user intending to do so.

In response to issues such as these, the "Smart Phone and Cloud Security Research Society"*[38] of Japan's Ministry of Internal Affairs and Communications summarized their interim report in December*[39], and published information on measures that should be implemented urgently to improve the information security level of smartphones.

■ Other Trends

The IPA issued a report analyzing targeted attacks, presenting the details of actual cases where emails were exploited in targeted attacks*[40]. The IPA also released a revision of their guidelines on "advanced persistent threats" and their handling as the "Design and Operational Guide to Cope with 'Advanced Persistent Threats' - 2nd Edition," at the same time as an English version of the first edition*[41].

*31 This malware was first discovered at the CrySyS research laboratory of a university in Hungary. Budapest University of Technology and Economics, Laboratory of Cryptography and Systems Security (CrySyS) "Duqu: A Stuxnet-like malware found in the wild" (http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf).

*32 The signatures used included a key stolen from a manufacturer in Taiwan and a code signing certificate stolen from a customer of Symantec. A detailed account can be found on the following Symantec Authentication (Business) Blog. "Duqu: Protect Your Private Keys" (http://www.symantec.com/connect/blogs/duqu-protect-your-private-keys).

*33 Microsoft patched this vulnerability in their December 2011 update. "Microsoft Security Bulletin MS11-087 - Critical: Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2639417)" (http://technet.microsoft.com/en-us/security/bulletin/ms11-087).

*34 Kaspersky Lab SECURELIST Blog, "Massive DNS poisoning attacks in Brazil" (http://www.securelist.com/en/blog/208193214/Massive_DNS_poisoning_attacks_in_Brazil).

*35 Premium SMS is a billing system using SMS (Short Message Service). Normally billing occurs when users reply to a billing confirmation message.

*36 F-Secure Blog, "Impostor Apps in the Android Market" (http://www.f-secure.com/weblog/archives/00002286.html).

*37 See the following blog post by the discoverer for more information. Android Security Test, "CarrierIQ" (http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/).

*38 Ministry of Internal Affairs and Communications, "'Smart Phone and Cloud Security Research Society' to be Initiated " (http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/111011_a.html).

*39 Ministry of Internal Affairs and Communications, "Official Announcement of Interim Report from 'Smart Phone and Cloud Security Research Society'" (http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/11121902.html).

*40 IPA, "IPA Technical Watch: Report on 'Analysis of Targeted Attack Email'" (http://www.ipa.go.jp/about/technicalwatch/20111003.html) (in Japanese).

*41 IPA, "Design and Operational Guide to Cope with 'Advanced Persistent Threats'" (http://www.ipa.go.jp/security/vuln/newattack.html) (in Japanese). An English version of its first edition is available at the following location. (http://www.ipa.go.jp/security/vuln/documents/eg_newattack.pdf)

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 October 1 and December 31, 2011. This information shows traffic anomalies judged to be attacks based on IIJ DDoS Defense Service standards. IIJ has also responded 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*[42], attacks on servers*[43], 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 450 DDoS attacks. This averages to 4.9 attacks per day, indicating a decrease in the average daily number of attacks compared to our prior report. Bandwidth capacity attacks accounted for 0% of all incidents, server attacks accounted for 79.3%, and compound attacks accounted for the remaining 20.7%.

The largest attack observed during the period under study was classified as a compound attack, and resulted in 157Mbps of bandwidth using up to 31,764pps packets over the course of 14 hours and 10 minutes. Of all attacks, 86.7% ended within 30 minutes of commencement, 11.8% lasted between 30 minutes and 24 hours, and 1.5% lasted over 24 hours. The longest sustained attack was a server attack that lasted for 39 hours and 26 minutes. The ratio of compound attacks was much higher in December than other months. This is due to continued attacks mostly originating from China on certain targets.

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*[44] and botnet*[45] usage as the method for conducting DDoS attacks.

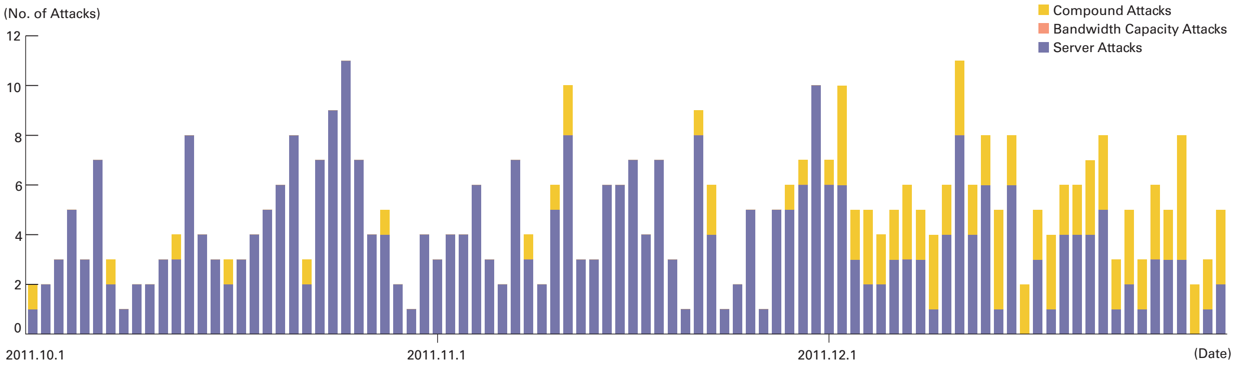


Figure 2: Trends in DDoS Attacks

*[42] 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.

*[43] 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.

*[44] 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.

*[45] 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*46 set up by the MITF, a malware activity observation project operated by IIJ*47. 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 October 1 and December 31, 2011, 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 53.7% of the total during the target period. Attacks on 3389/TCP used for remote desktop, 1723/TCP used for PPTP-based remote access VPN, and 21/TCP used by FTP were also observed. Looking at the origin of backscatter thought to indicate IP addresses targeted by DDoS attacks by country in Figure 3, China and the United States accounted for large proportions at 36.6% and 29.1%, respectively, with other countries following in order.

Regarding particularly large numbers of backscatter packets observed, there was an attack on the Web server (80/TCP) for a Chinese-language news site in the United States on October 7. Between October 14 and 19 attacks targeting 46045/TCP and 46049/TCP were also observed on a server in China. Many attacks targeting 80/TCP were observed on October 25. These attacks targeted a server in China and the Web server for a video streaming site in the British Virgin Islands. Intermittent attacks on the latter Web server (80/TCP) were observed between October and November. Many attacks on 80/TCP were also observed on November 23, with most targeting IP addresses held by a hosting provider in the United States. A series of attacks were also observed on the Web server (80/TCP) of an online store in the United States from late October until just before Christmas.

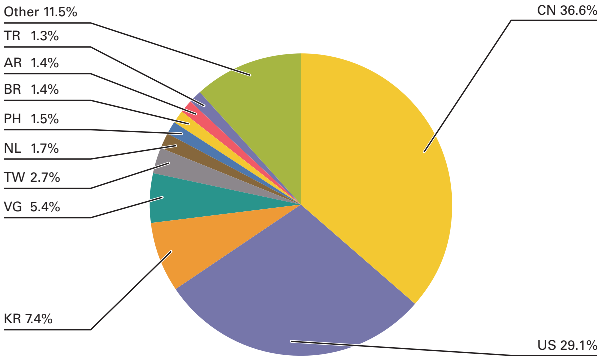


Figure 3: DDoS Attack Targets by Country According to Backscatter Observations

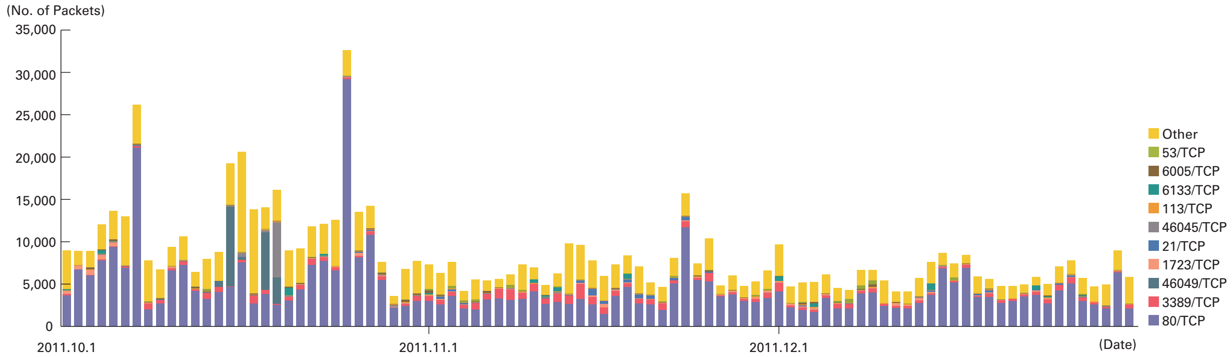


Figure 4: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)

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

*47 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).

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the MITF*[48], a malware activity observation project operated by IIJ. The MITF uses honeypots*[49] 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 October 1 and December 31, 2011. 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 communications targeting 1433/TCP used by Microsoft's SQL Server, 3389/TCP used by the RDP remote login function for Windows, and 4899/TCP used by the RAdmin remote management software for Windows, as well as scanning behavior for 22/TCP used for SSH. Additionally, communications of an unknown purpose were observed on ports not used by common applications, such as 2582/TCP and 26723/TCP. Looking at the overall sender distribution by country in Figure 5, we see that attacks sourced to China at 23.9%, Japan at 9.9%, and the United States at 9.0% were comparatively higher than the rest.

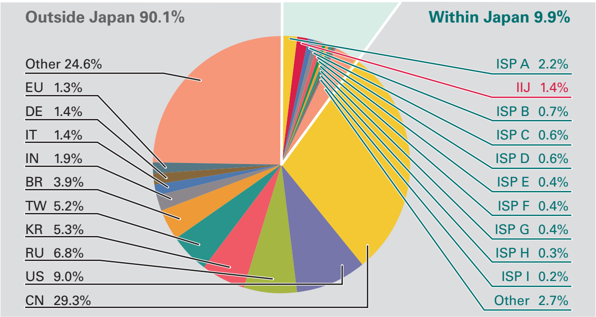


Figure 5: Sender Distribution (by Country, Entire Period under Study)

Communications thought to be SSH dictionary attacks also occurred intermittently. For example, concentrated communications were observed coming from IP addresses in the United States on October 7, South Korea on November 16 and 21, China on November 30, and South Korea and China on December 23. From November 4 2582/TCP communications were no longer observed. Although the reason for this is not known, because 95.6% of 2582/TCP communications come from within Japan, we believe that these communications come from a Japan-only application. RDP has started to show up in the top 10 since the heightened activity of the Morto worm that was detailed in the previous volume of this report. For the current survey period the majority of connections were from China.

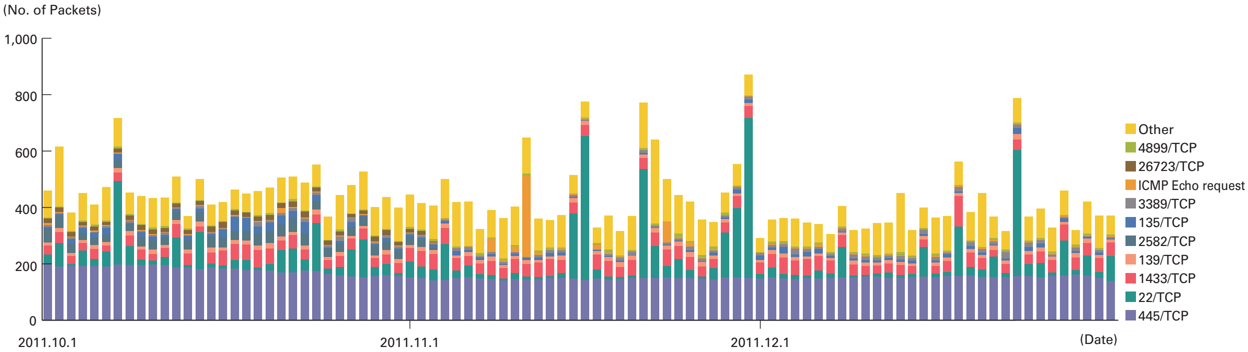


Figure 6: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

*48 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.

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

Malware Network Activity

Figure 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*[50], while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*[51]. 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 7, 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, 343 specimens were acquired per day during the period under study, representing 32 different malware variants. In Figure 7, specimens acquired from Thailand and Indonesia accounted for a large proportion at 35.9% and 17.5%, respectively.

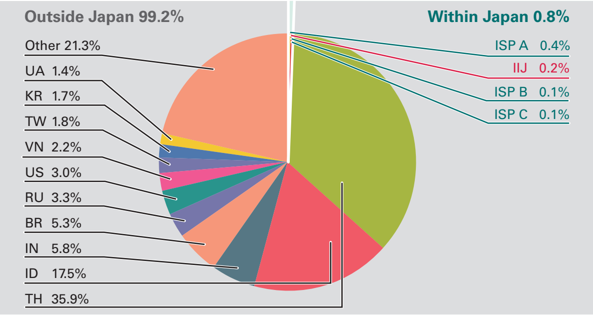


Figure 7: Distribution of Acquired Specimens by Source (by Country, Entire Period under Study, Excluding Conficker)

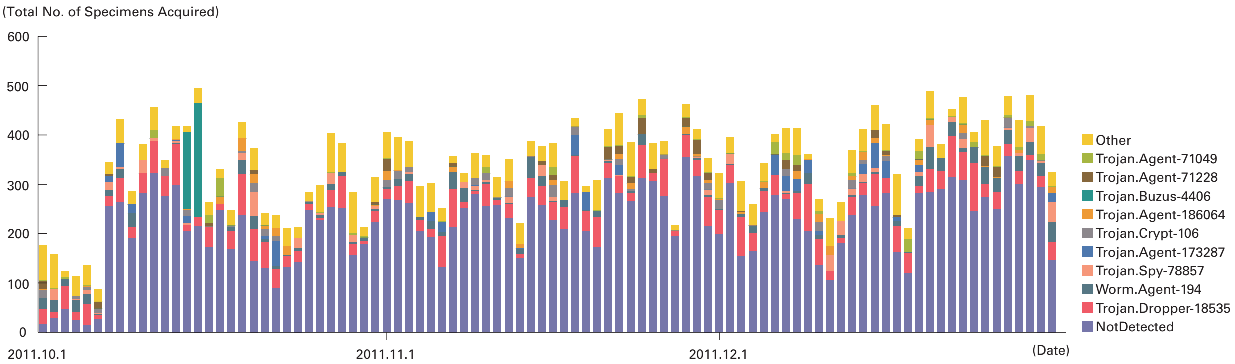


Figure 8: Trends in the Number of Malware Specimens Acquired (Excluding Conficker)

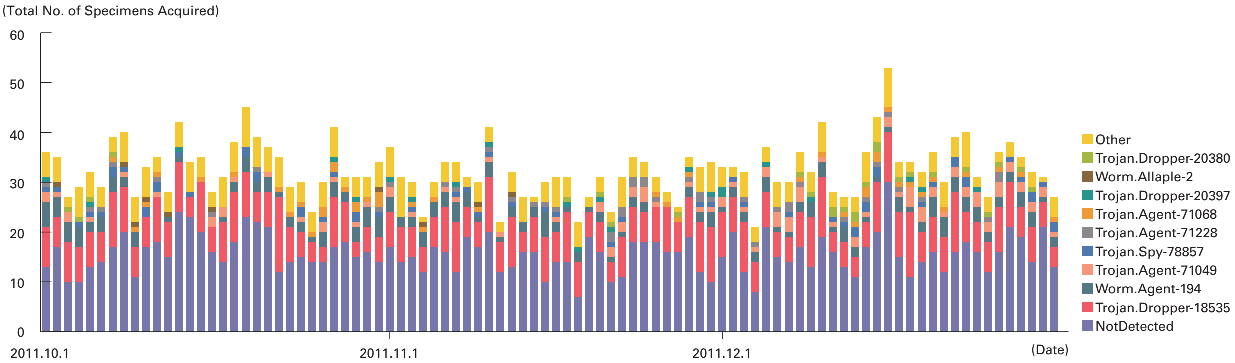


Figure 9: Trends in the Number of Unique Specimens (Excluding Conficker)

*[50] This indicates the malware acquired by honeypots.

*[51] 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.

Under the MITF's independent analysis, during the current period under observation 66.7% of malware specimens acquired were worms, 25.3% were bots, and 8.0% were downloaders. In addition, the MITF confirmed the presence of 21 botnet C&C servers*[52] and 17 malware distribution sites.

An Increase in Unknown Specimens from Thailand and Indonesia

The large ratio of unknown specimens (Not Detected) observed after October 7 in Figure 10 were mostly obtained from Thailand and Indonesia, with Thailand accounting for 55.4% and Indonesia for 26.4%. A breakdown of these specimens showed that 93.4% were executable files, and 6.6% were text format files such as HTML or XML.

After a more detailed examination, we learned that two types of bots*[53]*[54] controlled by IRC servers had been active. Classification by hash value showed that individual specimens were only active for a short period of one or two days.

Conficker Fluctuation

Figure 11 shows trends in the total number of malware specimens acquired for the same period including Conficker. The ratio for Conficker remained high at 99.3% of the overall total. The results of Conficker observations over an extended period of time demonstrate that it is still very active, with activity increasing and falling in cycles. During the current survey period an upward trend was noticeable in regions such as Russia, Brazil, and Taiwan, but there were no fluctuations evident in Japan or the United States. This shows that its activity differs based on the IP addresses allocated to each country.

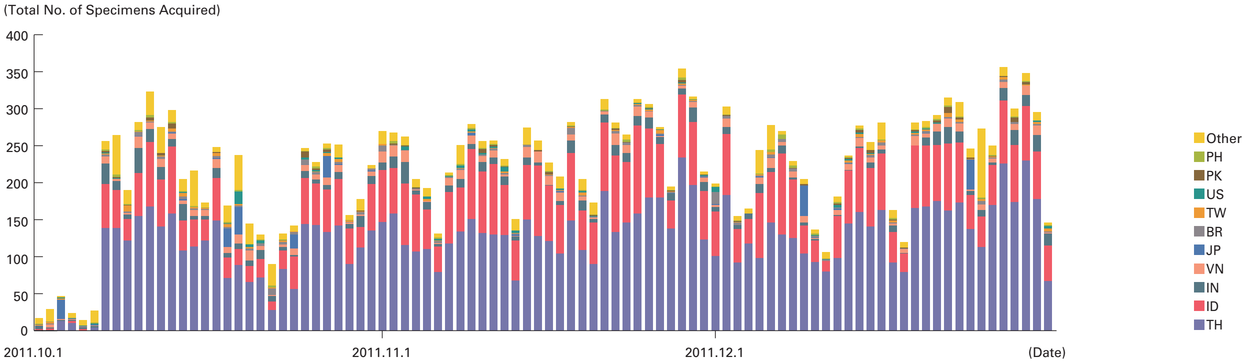


Figure 10: Trends in the Number of Malware Specimens Acquired (Unknown Specimens by Country)

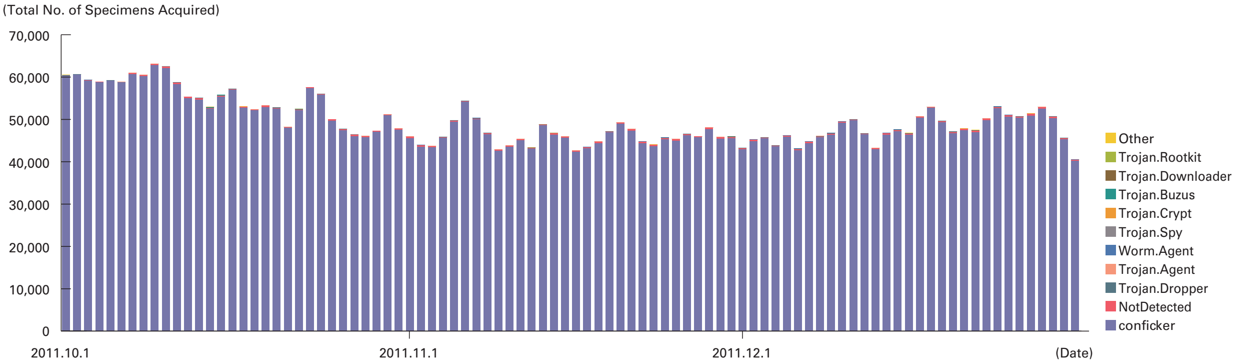


Figure 11: Trends in the Total Number of Malware Specimens Acquired (Including Conficker)

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

*[53] Trojan: Win32/Ircbrute (http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?name=Trojan%3AWin32%2FIrcbrute).

*[54] Win32/Hamweq (http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fHamweq).

1.3.3 SQL Injection Attacks

Of the different types of Web server attacks, IIJ conducts ongoing surveys related to SQL injection attacks*[55]. SQL injection attacks have flared up in frequency numerous times in the past. SQL injections are known to occur in one of three attack patterns: those that attempt to steal data, those that attempt to overload database servers, and those that attempt to rewrite Web content.

Figure 12 shows the distribution of SQL injection attacks against Web servers detected between October 1 and December 31, 2011. Figure 13 shows trends in the numbers of attacks. These are a summary of attacks detected by signatures on the IIJ Managed IPS Service.

Japan was the source for 48.2% of attacks observed, while China and the United States accounted for 16.0% and 9.0%, respectively, with other countries following in order. 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, the attacks that occurred on October 10 were from a specific attack source in the United States and directed at a specific target. A series of attacks that occurred between November 30 and December 2 were mainly from multiple attack sources in China and directed at multiple targets. Both of these incidents used the same attack techniques repeatedly, and are thought to have been attempts to find a vulnerability on a Web server.

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

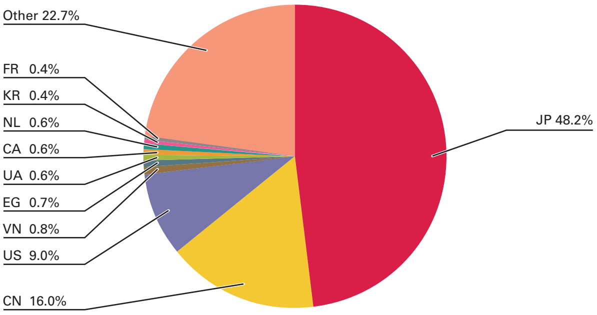


Figure 12: Distribution of SQL Injection Attacks by Source

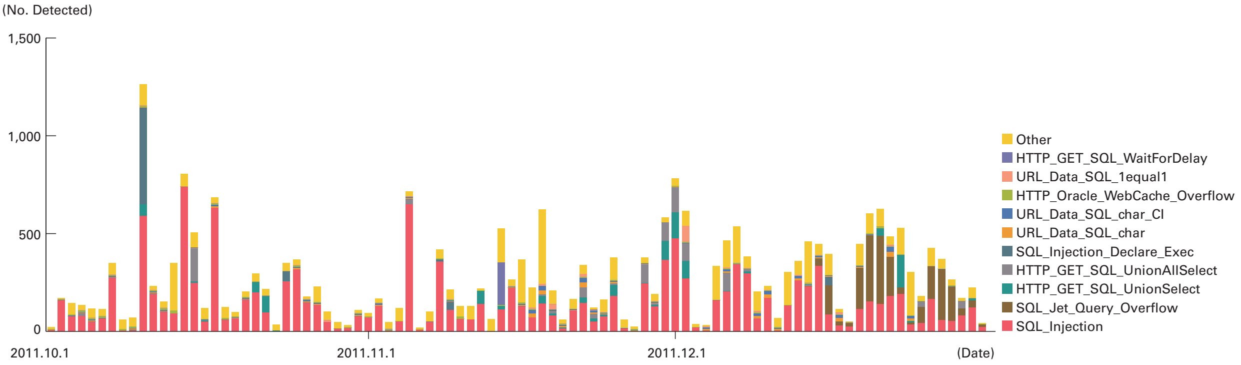


Figure 13: Trends in SQL Injection Attacks (by Day, by Attack Type)

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

1.4 Focused Research

Incidents occurring over the Internet change in type and scope from one minute to the next. Accordingly, IIJ works toward implementing countermeasures by continuing to perform independent surveys and analyses of prevalent incidents. Here we will present information from the surveys we have undertaken during this period regarding incidents related to the issuing of public key certificates, as well as targeted attacks and their handling.

1.4.1 Problems Related to the Issuing of Public Key Certificates

In this section we examine a hacking incident at another certificate authority similar to those detailed in the previous report*[56], discuss signed malware resulting from issuing policy problems at certificate authorities, and take a look at measures taken by the industry to resolve these issues in PKI (Public Key Infrastructure).

■ Fraudulent Issue Incidents Detailed in the Previous Volume

DigiNotar filed for bankruptcy in September 2011 due to the incidents that came to light in August. In initial press their earnings for the first half of the year from certificate authority work were reported as under 100,000 Euros, and it was thought that they had not been significantly impacted by the hacking incident. However, their liabilities were estimated at between 33 and 48 million U.S. dollars, so the loss of trust as a certificate authority had an extremely large effect on their operations*[57].

GMO GlobalSign, which was named by ComodoHacker as a system that was accessible without authorization, suspended the issuing of new certificates from September 6 to 15 in order to investigate. They also reset the passwords for all customer accounts upon resuming service. In a final report published in December it was announced that the certificate issuing system was not affected, but it took until mid-October for them to resume normal operations for all services*[58].

■ Hacking Incident at a Dutch Certificate Authority

In November 2011 a Dutch certificate authority service called Gemnet operated by KPN suspended the issuing of certificates due to the discovery of evidence that their certificate issuing system had been hacked*[59]. It was reported that according to the server log the hacking had taken place over 4 years ago*[60]. Following a report on November 4, the issuing of certificates was partially resumed from November 9.

KPN issues certificates both for general users and government entities. As with the DigiNotar hacking incident, the fact that they were accredited as one of the certificate authorities used by the Dutch government has been called into question*[61]. In fact, many of the organizations affected by the fraudulent issuing incidents at DigiNotar had switched to certificates issued by KPN*[62].

■ Issuing Policy Problems at a Malaysian Certificate Authority

In November 2011 it was discovered that Malaysian certificate authority DigiCert Sdn. Bhd. had issued certificates with weak 512-bit RSA keys and certificates that did not contain an Extended Key Usage extension. Entrust reported that these certificates were in violation of the CPS (Certification Practice Statement)*[63]. There were 22 certificates with weak keys, and DigiCert Sdn. Bhd. implemented a policy to replace certificates that had a 512- or 1024-bit RSA key issued by the intermediate CA (Distinguished Name: Digisign Server ID - (Enrich)) the problem had originated at with 2048-bit versions.

*56 IIR Vol.13 "1.4.3 Incidents of the Fraudulent Issue of Public Key Certificates" (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol13_EN.pdf).

*57 SANS ISC Diary, "Diginotar declared bankrupt" (http://isc.sans.edu/diary.html?storyid=11614).

*58 GMO GlobalSign, "Notice of the Resumption of Normal Operations" (http://jp.globalsign.com/information/important/2011/10/388.html) (in Japanese).

*59 KPN, "KPN stopt uit voorzorg uitgifte nieuwe veiligheidscertificaten" (https://www.kpn.com/corporate/overkpn/Newsroom/nieuwsbericht/KPN-stoptuit-voorzorg-uitgifte-nieuwe-veiligheidscertificaten.htm) (in Dutch).

*60 SANS NewsBites - Volume: XIII, Issue: 89, "Dutch Telecom KPN Halts SSL Certificate Issuing (November 4, 6 & 7, 2011)" (http://www.sans.org/newsletters/newsbites/newsbites.php?vol=13&issue=89&rss=Y#sID300).

*61 The Dutch ministry in charge of electronic communications, OPTA, has created a list of trusted certificate authorities. OPTA "Trusted Service List" (https://www.opta.nl/en/tsl/).

*62 Kaspersky Lab, "Malware in November: Parallels Between Duqu and Stuxnet and a Lack of Trust in Certificate Authorities" (http://www.kaspersky.com/about/news/virus/2011/Malware_in_November_Parallels_Between_Duqu_and_Stuxnet_and_a_Lack_of_Trust_in_Certificate_Authorities).

*63 "Entrust Bulletin on Certificates Issued with Weak 512-bit RSA Keys by Digicert Malaysia" (http://www.entrust.net/advisories/malaysia.htm).

Meanwhile, even before DigiCert Sdn. Bhd. initiated measures to resolve the problem, the overseeing root certificate authority Entrust implemented a policy of revoking the certificate of the intermediate CA by November 8 at the latest. These stringent measures are thought to have been taken in light of the failures of DigiNotar and others.

The problems exposed at DigiCert Sdn. Bhd. were not due to incidents of fraudulent issuing as was the case with Comodo or DigiNotar. However, the impact is the same for users of certificates that need to verify their reliability. It is likely that general users usually verify the reliability of certificates via browsers using SSL/TLS communications. This means that it has been necessary for major browser vendors to revoke certificates from intermediate CAs and their subordinate certificates in response to incidents such as this, or in other words create a black list to prohibit the use of the affected certificates.

There were three separate problems with the certificates revoked in this case. We discuss each of these problems below.

■ Problem 1: The Compromise of Cryptographic Algorithms and Public Key Length

Under standard certificate issuing procedures, when a party requests the issue of a certificate, application data known as a CSR (Certificate Signing Request) is submitted to a certificate authority. When a certificate authority issues a certificate, they check the public key and X.509 Distinguished Name included in the CSR. It has been noted that the recent problems were caused because the certificate authority had no policy regarding key length, and also did not check key length*[64]. Additionally, by searching the EFF SSL Observatory*[65] public key certificate database maintained by the EFF (Electronic Frontier Foundation), it was discovered that certificate authorities other than DigiCert Sdn. Bhd. had also issued certificates with 512-bit RSA public keys. One reason that 512-bit RSA public keys cannot be relied upon for signatures or encryption is that prime factorization of a 768-bit RSA public key has already been demonstrated*[66]. 1024-bit RSA public keys are also currently used, but transition to 2048-bit keys is recommended.

Emergency measures taken by DigiCert Sdn. Bhd. focused only on the key length of the RSA encryption algorithm, but with regard to the compromise of cryptographic algorithms*[67], consideration should also be given to the hash function algorithm used in digital signatures. Specifically, with the compromise of MD5, recognition of the fact that certificates digitally signed using MD5 are already not safe is spreading. It has been pointed out that the currently predominant SHA-1 is also weak, and the transition to root certificates with signatures using SHA-2 is progressing. Both servers and clients must be updated for transition, but web server upgrades, certificate trials, and the installation of SHA-2 root certificates on mobile phones have been reported, indicating that transition is proceeding steadily.

Regarding transitioning the use of cryptographic algorithms*[68], NIST published SP 800-131A with a partially revised transition plan that provides specific guidelines for each cryptographic algorithm. In addition to listing corresponding algorithms (and key lengths) as Acceptable and Disallowed, this document also defines Deprecated (usable if risks are acceptable) and Restricted statuses, with status designed to change over time.

■ Problem 2: Use for Purposes other than Originally Intended

It was reported that one of the certificates issued to Malaysian government-related organization domain anjungnet.mardi.gov.my by the intermediate CA that problems were identified at was used to sign malware that exploited a vulnerability in Adobe Reader*[69]. By the time of this report the certificate had already expired, but between its signing on August 24 and its expiry on September 29 there is a chance that malware was installed without warning even on OSes with a signature verification function.

*64 FOX-IT, “RSA-512 Certificates abused in the wild” (http://blog.fox-it.com/2011/11/21/rsa-512-certificates-abused-in-the-wild/).

*65 The EFF SSL Observatory (http://eff.org/observatory). This project collects a wide range of public key certificates used on HTTPS servers. The data set is published to monitor whether there are problems with certificates issued by CA. These activities were first detailed at DEFCON18 held in July 2010 (https://www.eff.org/files/DefconSSLiverse.pdf).

*66 Thorsten Kleinjung et.al, “Factorization of a 768-bit RSA modulus” (http://eprint.iacr.org/2010/006).

*67 The compromise of cryptographic algorithms is discussed in IIR Vol.8 under “1.4.1 Trends in the Year 2010 Issues on Cryptographic Algorithms” (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol08_EN.pdf).

*68 NIST, “SP800-131A Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, January 2011” (http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf).

*69 F-Secure Blog, “Malware Signed With a Governmental Signing Key” (http://www.f-secure.com/weblog/archives/00002269.html).

It has been pointed out that the fact the certificates used 512-bit RSA public keys and also had no restrictions on its usage created a two-fold problem*[70]. Systems for restricting the usage of certificates include the Extended Key Usage X.509 v3 extension. This extension is defined in RFC5280, and makes it possible to restrict usage by describing the intended use such as SSL, code signing, or S/MIME in a certificate. By setting these restrictions, or in others words restricting server certificates to their original purpose of SSL communications, use for purposes other than those intended can be detected during verification, making it possible to protect against the installation of malware.

■ Problem 3: Lack of Revocation Information References in Certificates

Public key certificates have expiration dates set to lessen the impact of cryptographic compromises due to continued use of the same public key and to support the PKI business model. The certificates related to a private key are usually used for one to several years, with some root certificates used for over ten years in consideration of the cost of replacing trust anchors. Meanwhile, a system for revoking certificates before they expire is also in place. Reasons for revoking a certificate include the leaking of the private key, with CRL (Certificate Revocation List: data listing the serial numbers for certificates to revoke before expiry signed by the CA) that also allows verification offline and OCSP (Online Certificate Status Protocol: a protocol defined in RFC2560 for confirming whether a certificate has been revoked online) both widely used.

Normally CRL-related information is described in the CRL Distribution Points extension, and OCSP-related information in the Authority Information Access extension, as defined in the aforementioned RFC5280. The certificates that caused problems in this case contained no information about methods for confirming their validity. For this reason, although the certificate authority announced the corresponding certificates had been revoked, it is not possible to check whether certificates have been revoked in applications such as browsers. The fact that a revoked certificate can still be accepted and processed is seen as a problem.

■ Restoring Overall Confidence in the PKI Industry

In November 2011 when the incidents at KPN and DigiCert Sdn. Bhd. detailed here occurred, activities for restoring overall confidence in the PKI industry were announced. This refers to the baseline requirements*[71] adopted by the CA/Browser Forum, which is planning EV SSL certificates that will be issued under unified industry standards*[72] with stricter issuing reviews. This document was adopted on November 22, and is set to be enacted from July 2012. Companies participating in the forum are expected to implement the requirements during this preliminary period.

As with the issuing requirements for EV SSL certificates, these requirements prescribe cryptographic algorithm and key length restrictions, as well as normative restrictions regarding X.509 v3 extensions. Additionally, the restrictions prescribe the content that should be included in each of the Extended Key Usage, CRL Distribution Points, and Authority Information Access certificate extensions for resolving the issues described above. There are also regulations regarding the processing of these extensions that enable proper processing regardless of the service or product.

By defining baseline requirements for CA processes such as the issuing, verification, and revocation of certificates, it should be possible to equalize the variation in issuing requirements between each certificate authority. In addition to covering certificate issuing and verification functions, these requirements also touch upon employee training, log retention, system security risk assessment, and private key protection. Initiatives for restoring confidence in PKI business will continue to be carried out in the future.

*70 Entrust, "512-bit Certificates Abused in the Wild" (http://ssl.entrust.net/blog/?p=1041).

*71 CA/Browser Forum, "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.0, 22 Nov. 2011" (http://www.cabforum.org/Baseline_Requirements_V1.pdf).

*72 CA/Browser Forum, "Guidelines For The Issuance And Management Of Extended Validation Certificates ver1.3" (http://www.cabforum.org/Guidelines_v1_3.pdf).

1.4.2 Targeted Attacks and Their Handling

Targeted attacks have gained a lot of attention due to reports of a series of "cyber attacks" triggered by virus infections at major Japanese corporations discovered in September 2011. Security products and services providing measures against these attack methods have already appeared, with most focusing on targeted attack email and the malware exploited in particular. However, in some cases targeted attacks cannot be prevented by individual technological measures alone. Here we evaluate a wide range of measures by examining the attack process based on information about attacks that have been identified in the past.

■ Targeted Attacks and Their History

Targeted attacks are those that target a specific organization or individual. These incidents pose no threat of infecting random users like malware that spreads across the Internet by Web infection, and may only affect a single organization in the world at any one time. This makes it hard to ascertain the circumstances surrounding attacks, and the targeted organization is forced to face the problem alone.

Many attack methods involve exploiting email or IM software that is used on a day-to-day basis, and use messages containing topics of interests to users at the targeted organization (major news stories at the time of the attack, etc.) or appearing to be correspondence related to their work. These messages prompt users to open an attachment or access an external Web server, leading to malware infection. In order words, in many cases the first stage of an attack is to breach security boundaries such as firewalls at an organization by inserting malware into communications that users at the organization receive on a daily basis.

A hacker that has breached an organization's security boundary may first use the computer infected with malware to examine the internal network and locate the information they seek. In this case the Internet-based hacker will spend long stretches of time communicating with the infected computer within the organization.

Another characteristic of targeted attacks is the difficulty of sharing information about them. There are far fewer incidents than normal malware, and in some cases the affected party may decide not to share information externally because information indicating that an attack occurred may include details about the targeted organization. For this reason it is hard to ascertain the status of targeted attacks occurring in Japan or on the Internet as a whole, and except for a number of published incidents little is known about the attacks that have occurred and the damages that have been caused.

Meanwhile, these targeted attacks did not just appear abruptly last year, with published accounts going back as far as 2005*[73]. At the time that these attack methods were acknowledged almost all incidents targeted servers related to government agencies, and they were interpreted as part of espionage on a national scale. However, in the past few years cases where these attack methods have been used to target private-sector businesses have also been discovered.

■ The Targeted Attack Process

Table 1 summarizes typical cases of targeted attacks that have occurred over the past few years. Based on these incidents, we believe that the process for targeted attacks can be broken down into five stages: motivation, attack preparations, breaching of security boundaries, activity on the organization's network, and achievement of objectives. We explain each of these stages below.

■ Motivation

The objective of many targeted attacks is to steal information from the organization targeted. Most of the information targeted is corporate secrets, with the real purpose likely to be to exploit stolen information for monetary gain or competitive advantage. There are also attacks targeting information to use in attacks on other organizations*[74]. In an incident at EMC the ultimate target was organizations that use EMC products, and it is believed that stolen information was exploited in attempts

*73 For example U.S. US-CERT's "US-CERT Technical Cyber Security Alert TA05-189A - Targeted Trojan Email Attacks" (http://www.us-cert.gov/cas/techalerts/TA05-189A.html), or U.K. CPNI's "TARGETED TROJAN EMAIL ATTACK" (http://www.cpni.gov.uk/Documents/Publications/2005/2005015-BN0805_Targeted_trojan_ email.pdf).

*74 IPA, "Case Analysis and Countermeasure Report on Targeted Cyber Attacks" (http://www.ipa.go.jp/security/fy23/reports/measures/documents/report20120120.pdf) (in Japanese).

to attack other companies. Additionally, in an incident in Japan an industry group the targeted company was a member of was hacked in advance and stolen information used to send email with malware attached that appeared to be part of an email exchange between these two organizations.

Lastly, some attacks have been aimed at discrediting the targeted company. Anonymous claimed responsibility for an incident at HBGary Federal that was triggered by an attempt to publish the results of an investigation on Anonymous. In the end all email stored on their mail server was stolen and made available to the public. When this is the objective we can assume that the information stolen can be anything that embarrasses the target when the theft is made known.

■ Attack Preparations

Once a target is decided, attackers are likely to obtain information about the target in advance via a variety of methods. For example, invasion routes can be found by looking for vulnerabilities in systems exposed to the Internet, and public contact points or individual email addresses for the target organization can be learned by using search engines, etc., to identify targets for attack emails. Information about the applications used within an organization can also be used in attacks. If users at a targeted organization make their real names or organization they belong to known via SNS, it is sometimes possible to gain information on the applications used by examining their contact information or day-to-day comments. Additionally, for personnel with jobs that involve handing out business cards to many people such as sales staff, the information on their business cards is more likely to fall into the hands of an attacker.

Table 1: Examples of Targeted Attacks[*75]

Date	Overview	Method of Breaching Security Boundaries	Activity on the Organization's Network	Impact
November 2009	Night Dragon Several companies including energy-related companies involved in oil or natural gas and pharmaceutical companies.	Web server hacking and alteration originating from an SQL injection. Targeted attack emails that prompt users to access the altered content.	Installation of a RAT (zwShell). Hacking of management server. Repeated network exploration and attempts to hack other computers.	Corporate secrets such as information about operations and bids as well as email archives on a manager's computer were targeted.
January 2010	Operation Aurora Several dozen IT-related companies in the United States.	Email and IM messages containing an URL that leads users to Web infection malware.	Installation of malware controlled from a C&C server on the Internet.	Leaking of intellectual property and related information, including access to a source code management system.
February 2011	Attack on HBGary Federal by Anonymous.	Hacking via exploitation of CMS and server vulnerabilities and the reuse of passwords.	Hacking of internal servers by exploiting vulnerabilities in the internal system and asking for IDs and passwords in email exchanges.	Leaking of corporate secrets (email archive). Discrediting the company by publishing leaked information to the Internet.
March 2011	Attack on EMC.	Targeted attack email sent to general users disguised as being related to a recruitment plan.	Network exploration exploiting a RAT (Poison Ivy). Authentication information was acquired and company servers were repeatedly hacked.	Leaking of secrets regarding company products. Attacks on other companies exploiting these secrets.
April to September 2011	Nitro Attacks Multiple companies including human-rights organizations and automotive, chemical, and defense industry companies.	Targeted attack email disguised as either a software security update or an invitation to a business gathering.	Installation of a RAT (Poison Ivy) to computers. Discovery of computer information (including password hashes) and hacking of neighboring computers and management servers.	Corporate secrets such as product manufacturing processes were targeted.

[*75] Information on each of the attacks is summarized below.
Night Dragon: MacAfee, Inc., "Global Energy Cyberattacks: 'Night Dragon'" (http://www.mcafee.com/ca/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf). Operation Aurora: HBGary, "HBGary Threat Report: Operation Aurora" (http://hbgary.com/hbgary-threat-report-operation-aurora), and IIR Vol.07 "1.4.2 Targeted Attacks and Operation Aurora" (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol07_EN.pdf).
HBGary Federal: "Anonymous speaks: the inside story of the HBGary hack" (http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars/).
EMC: Sophos, nakedsecurity, "RSA release a few details on their big security breach" (http://nakedsecurity.sophos.com/2011/04/04/rsa-release-details-on-security-breach/).
Nitro Attacks: Symantec, "The Nitro Attacks Stealing Secrets from the Chemical Industry" (http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf).

Breaching of Security Boundaries

Security boundaries are breached by exploiting information about the target learned in advance to attempt to hack the organization’s network. Email or instant messenger messages containing text disguised as work-related information or text including topics that attract broad interest are sent, leading users on the organization’s network that receive these messages to be infected with malware*[76]. It is known that the Nitro Attacks incident originated from an email disguised as a security update alert for Adobe products sent to general users, while for the EMC incident email disguised as information related to the recruitment plan for the following year was sent. The number of people that targeted attack email or messages are sent to varies for each incident. Regardless of the volume sent, if even one recipient is infected with malware, the attacker secures a foothold for attacking the organization’s network, and can move on to the next stage.

Some incidents also originate from attacks that exploit vulnerabilities in servers exposed to the Internet. For Night Dragon an SQL injection was used, and for HBGary Federal CMS and server OS vulnerabilities and the reuse of IDs and passwords between multiple systems were exploited.

Activity on the Organization’s Network

Except when information about the configuration and internal systems of an organization’s network have been obtained in advance, once a network is hacked the attacker will attempt to hack a more critical system or the computer of a more important individual, such as personnel with administrator privileges or a manager. To achieve this they obtain and exploit email and authentication information saved to the computers they have hacked, and attack authentication servers or network resources such as management servers. In fact, several of the incidents presented in Table 1 and many incidents occurring in Japan are thought to have involved attacks on an Active Directory server managing an organization’s network to gain administrator privileges or steal all user IDs and passwords.

Other examples of attacks that had repercussions on an organization’s network include reports of attacks on mail servers (including archived mail) and file servers (to steal important files or use as a base to infect an organization with malware).

These incidents do not always involve malware programmed to attack an organization’s network in advance. Sometimes the status of an organization’s network is investigated in a more manual way by exploiting malware such as RAT*[77] to send a sequence of commands from the Internet. In this case communications between the Internet-based attacker and the hacked computer take place frequently and over an extended period of time. Attackers are known to use communications normally seen on computers (HTTP, SSL, SMTP, DNS) to prevent them being blocked by the security boundary or detected immediately.

Achievement of Objectives

Once an attacker has found the information they are looking for using the above process, they send it to the Internet. In a number of cases attackers have been known to collect large amounts of information stolen from hacked servers, upload it to an FTP server on the Internet, and later delete any traces left on the FTP server. In other cases information has been leaked by sending it via email to an external email address.

Linked Targeted Attacks

Email-based targeted attacks consist of two distinct types. The first involves sending emails to multiple individuals at multiple organizations, and the second involves targeted attack emails sent to an extremely limited number of people. For example, while in the Nitro Attacks incident an email disguised as a security update alert for Adobe products was sent to between 100 and 500 users at each company, another email disguised as an invitation to a business gathering was apparently only sent

*76 Examples of targeted attack email from incidents in Japan can be found in the following IPA report. IPA Technical Watch, “Report on ‘Targeted Attack Email Analysis’ - 4 Examples of Fraud Techniques Used and Analysis/Countermeasures for Targeted Attack Email” (http://www.ipa.go.jp/about/technicalwatch/20111003.html) (in Japanese).

*77 RAT is an abbreviation of Remote Access Trojanhorse or Remote Access Tool, indicating tools for controlling computers remotely. Common examples include Gh0st RAT and Poison Ivy. In targeted attacks these tools are often used either as-is or in modified form to control computers on an organization’s network (See examples under “Activities on the Organization’s Network” in Table 1).

to a few individuals. As indicated in the description of the targeted attack process above, this difference can be explained by the fact that attackers sometimes carry out targeted attacks to obtain information for use in a separate targeted attack (Figure 15).

Usually it is difficult for attackers outside an organization to learn the contact details for individuals close to the information they seek, for example an administrator with elevated privileges or a manager with access to classified company information. To obtain this information attackers first launch a targeted attack on general users at the target organization or on a related organization by sending an email with content that catches the interest of a wide range of people.

Once they obtain information about the target, the next targeted attack is carried out. For these attacks the information previously obtained is used to target just a few individuals. For example, a reply is sent quoting the text of an email from someone with whom messages are exchanged regularly. To the recipient of the targeted attack email this appears to simply be the continuation of a work-related discussion, and they are more likely to be infected with malware as a result.

There continue to be reports of targeted attacks on major corporations and organizations related to government offices, but the fact that these attacks come in different forms and have varying purposes must be taken into consideration. In other words, targeted attacks can affect even ordinary companies, and shouldn't be thought of as attacks that only target particular organizations.

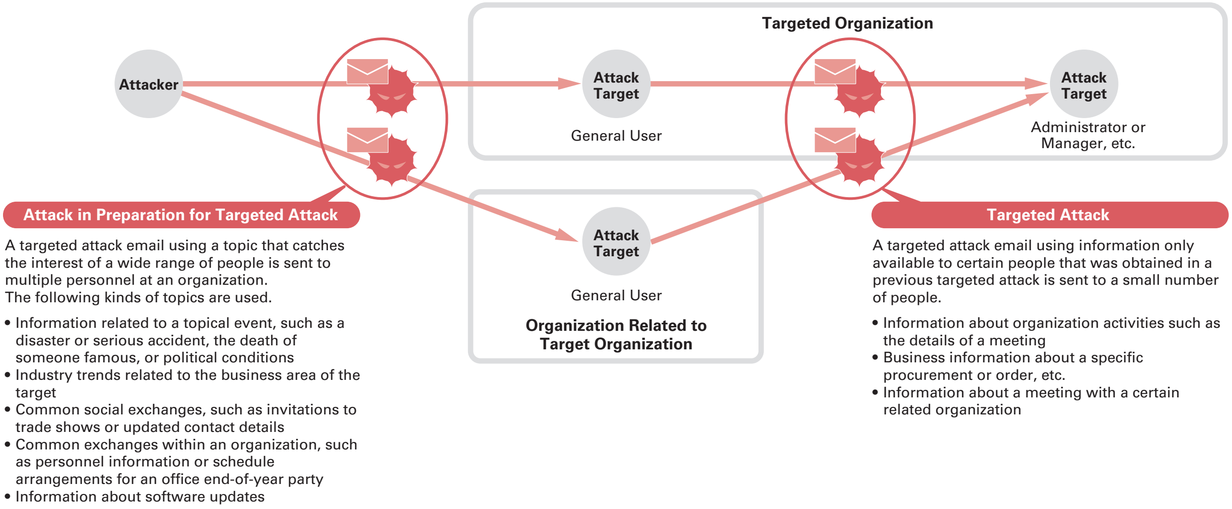
Evaluation of Targeted Attack Countermeasures

Lastly, we will evaluate targeted attack countermeasures based on the techniques and processes detailed above. Table 2 shows an overview of these evaluations.

Attack Preparation Countermeasures

First it is necessary to confirm any information about your organization available on the Internet that could be exploited. In addition to information published in DNS or WHOIS and publicly disclosed email addresses for contact points, check whether information about organization staff is available online via search engines or SNS, etc. Priority should be given to protecting systems or email addresses identified as exposed to the public, as they could be used as breach points in a targeted attack. Individuals that have fallen victim to a targeted attack in the past should also be similarly protected, as it is likely that some of their information is already in the hands of attackers.

You should also consider the possibility that organizations you have a working relationship with (industry groups, suppliers, vendors of systems you use) may be hacked, and information stolen from them exploited in an attack against your


Targeted Organization
Attacker
Attack Target
General User
Attack Target
Administrator or Manager, etc.
Attack Target
General User
Organization Related to Target Organization
Attack in Preparation for Targeted Attack
Targeted Attack

A targeted attack email using a topic that catches the interest of a wide range of people is sent to multiple personnel at an organization.
The following kinds of topics are used.

- Information related to a topical event, such as a disaster or serious accident, the death of someone famous, or political conditions
- Industry trends related to the business area of the target
- Common social exchanges, such as invitations to trade shows or updated contact details
- Common exchanges within an organization, such as personnel information or schedule arrangements for an office end-of-year party
- Information about software updates

A targeted attack email using information only available to certain people that was obtained in a previous targeted attack is sent to a small number of people.

- Information about organization activities such as the details of a meeting
- Business information about a specific procurement or order, etc.
- Information about a meeting with a certain related organization

The arrows in the figure indicate the route as presented to the target, and not the actual email delivery route. In some cases the email is misrepresented and sent directly from the attacker.
Targeted attack emails include those with content that catches the interest of a wide range of people, and those with content that can only be known by the parties concerned. For the latter type, information such as an email spool stolen in an earlier attack on said parties is exploited.
When an email containing information that can only be known to the parties concerned is received, it is difficult for the end target to determine from the content that it is a spoofed attack email. As this demonstrates, targeted attacks are not exclusively launched against government agencies or major corporations, and may also affect organizations related to those targeted.

Figure 15: Linked Targeted Attacks

organization. You can prepare for this kind of linked attack by confirming the security measures in place at organizations you have a working relationship with, and asking to be contacted if an incident occurs there*[78].

■ Inbound Measure Reinforcement

First, it is necessary to confirm whether there are any vulnerabilities in servers exposed to the Internet. Particular care must be taken with software that is updated frequently.

Many targeted attacks are carried out using spam or spoofed email, so introducing anti-spam measures can help to a certain extent. It is necessary to recommend the implementation of SPF or DKIM to organizations you need to exchange work-related email with, while introducing a system for verifying the signatures, etc., of email that is received at your organization.

You can also reduce the risk of attacks by coordinating with security providers and external organizations to obtain information about external servers used in targeted attacks, registering these to a black list, and blocking email from them.

■ Reinforcing Outbound Measures*[79]

Malware that infiltrates an organization sends information to the Internet and explores the organization's network via commands received from the Internet. When this takes place some form of communications occurs between the hacked

Table 2: Targeted Attack Countermeasures

Targeted Attack Countermeasures	Overview	Countermeasure Policy
Attack preparation countermeasures	Measures against vulnerabilities in exposed systems	Check the security of systems exposed to the Internet. Check whether there are vulnerabilities in software used, and whether IDs and passwords are reused.
	Confirmation of published information	Check the information about your organization that is available on the Internet. This includes email addresses, names of personnel, systems and versions used, etc. Reinforce security on the assumption that each piece of information available may be exploited in an attack.
	Security at other organizations	If you have a working relationship with other organizations, confirm the status of their security.
Security boundary breach countermeasures (inbound measure reinforcement)	Bolstering security of exposed systems	Isolate systems exposed to the Internet sufficiently so that the organization's network is not affected if the system is hacked.
	Countermeasures for spoofed email	Use solutions such as anti-spam technology to block spoofed email.
	Utilization of black lists	Create a black list of IP addresses, etc., used to send targeted attack email in the past to block email from them.
Security boundary breach countermeasures (outbound measure reinforcement)	Utilization of black lists for addresses malware connects to	Create a black list from information such as IP addresses that malware used in targeted attacks connect to, and prevent communications with these addresses from within the organization.
	Utilization of white lists	Restrict Internet access to trusted servers that are required for the work process.
Blocking activity on the organization's network	Protection of internal servers	Revise the protection of information necessary for operating the organization's network as well as the servers responsible for this information. Also review the protection of important servers such as mail and file sharing servers, as well as user access privileges.
	Protection of important information	Go over important information at the organization as well as methods for protecting it. Revise the handling of information at the organization based on the definition of important information, and restrict access methods to the absolute minimum necessary.
Knowledge regarding targeted attacks	Training	Give training on targeted attacks to users at the organization. Cover both the existence of attacks as well as the methods used, and recommend that email and messages not required for work purposes are deleted.
	Exercises	Send a mock targeted attack email to staff at the organization to examine how they react to targeted attacks, and repeat this exercise to raise their resistance to attacks.
Security operations and emergency response	Security operations	Implement a system for security operations such as abnormal behavior detection for operations on the organization's system. Use operation tools to collect information about security.
	Emergency response	Have emergency response capabilities in place at the organization for preserving and analyzing evidence and identifying the extent of impact after traffic anomalies or malware infections are detected.
Information sharing	Gathering information regarding targeted attacks	Gather information about targeted attacks that occur at other organizations by participating in information sharing projects, etc. It is particularly important to obtain the addresses, malware, and message text used in attacks on other organization to apply them to inbound and outbound black lists, and to alert users.

*78 For example, the National Information Security Center indicates that one of the "measures regarding information sharing, etc. that the government should consider to combat targeted attacks" is including maintenance of an information security framework, maintenance of confidentiality, notification of security breaches, and implementation of audits in the information security requirements for suppliers during procurement. 28th assembly of the Information Security Policy Council (January 24, 2012) Reference 1-1 "Public-Private Coordination Regarding Information Security Measures" (http://www.nisc.go.jp/conference/seisaku/dai28/pdf/28shiryou1-1.pdf) (in Japanese).

*79 Outbound measures are a concept introduced in the following IPA guide. These measures block malware activity using a combination of the existing security boundary system and the results of malware behavior analysis. IPA, "Design and Operational Guide to Cope with 'Advanced Persistent Threats'" (http://www.ipa.go.jp/security/vuln/documents/eg_newattack.pdf).

computer and the Internet-based attacker. You can prevent information leaks and stop commands being received by blocking these communications. Malware communications uses communications protocols such as HTTP, SSL, or SMTP that are allowed for connections to the Internet at many organizations. This means that to block malware communications it is first necessary to create and implement a policy for setting restrictions on Internet communications from within the organization.

This can be done with the firewall, IPS, or HTTP proxy used to secure an existing security boundary. For example, by obtaining information about the connections made by malware used in targeted attacks from anti-virus vendors or security providers, and registering this to a black list, you can prevent communications with the corresponding servers from within the organization's network. If the work carried out by the organization permits it, you can also block a wider range of malware communications by operating a white list that limits connections to specific trusted servers.

■ Blocking Activity on the Organization's Network

In many cases, the hacking of a general user's computer leads to the hacking of other computers or servers on the organization's network. Considering the volume of information that can be obtained if a hack is successful, management servers on the organization's network are likely to be targeted next*[80]. Because many management servers have no protection against attacks from other computers on the organization's network, it is necessary to limit communications between computers and management servers, and implement security devices capable of interpreting management protocols to prepare for attacks on servers from other computers.

By setting multiple security boundaries on an organization's network it is possible to prevent attackers from reaching important information even if they manage to breach part of the network. An example of this is preventing the computers of general users from communicating with systems containing important information. It is particularly important to set boundaries and authentication so that attackers do not have the privileges to reach important information when a management server is breached.

■ Knowledge Regarding Targeted Attacks

When a general user at an organization receives a targeted attack email, the handling of this email determines whether that organization is strong or vulnerable against targeted attacks. For example, organizations that only allow work-related email to be handled are more resistant against attacks than organizations that allow email unrelated to day-to-day work.

If users are aware of targeted attacks, know that many are carried out using email, and understand trends such as spoofing and the kind of text used, it will lower the chance that they will be infected with malware by opening attachments or clicking URLs when they receive a targeted attack email. Effective methods for providing this kind of knowledge to general users include company training and exercises using mock targeted attack emails within an organization.

■ Security Operations and Emergency Response

By constantly monitoring communications from within an organization to the Internet, and implementing a system for detecting abnormal traffic such as large volumes of communications to a certain address, you can detect communications between malware that has infiltrated the organization and a server on the Internet. A system for extracting meaningful security information from day-to-day operations on an organization's network should be evaluated.

The emergency responses required when an abnormality is detected include preserving the computer carrying out communications, investigating malware infections, analyzing malware specimens, examining connections and the content of communications, setting up a workaround for blocking malware communications, identifying the malware infection route, checking for attacks on other computers or servers, and confirming whether information has been leaked. Preparations should be made to ensure these functions are implemented within the organization*[81].

*80 Because management servers have been targeted in some cases, the National Information Security Center has issued an alert to ministries and agencies. NISC, "Regarding Thorough Security Measures for Servers that Manage Network Users" (http://www.nisc.go.jp/active/general/pdf/ada_kanki_111222.pdf) (in Japanese).

*81 The previously mentioned "Public-Private Coordination Regarding Information Security Measures" reference material from the 28th assembly of the Information Security Policy Council also calls for the establishment of an emergency response team (CSIRT) for performing these kinds of functions at all government institutions in Japan.

Information Sharing

With several targeted attacks having come to light in quick succession, a number of information sharing projects have now been set up in Japan to evaluate countermeasures for targeted attacks based on knowledge accumulated from past incidents. By participating in one of these projects it is possible to implement countermeasures based on information about targeted attacks that have taken place at other organizations.

Meanwhile, those who participate in this kind of project are sometimes also expected to provide information about targeted attacks they have experienced. Some organizations are adverse to making information about attacks that have occurred to them public even to a limited extent. For this reason some projects share information under a strict NDA, and other projects are debating the incentives for sharing information.

The inbound measures such as access control using a black list of senders and outbound measures for malware communications that we have introduced here depend on knowledge about targeted attacks that have already occurred, and cannot be implemented unless information is shared. We believe that to cope with the current situation in which the damages from targeted attacks are ongoing it is necessary for one of the many information sharing projects currently being evaluated to emerge as dominant*[82].

Summary

As we have demonstrated here, targeted attacks are not a singular problem but a compound problem that begins when an organization is targeted. Dealing with these attacks requires an effective combination of multiple measures rather than a simple stopgap.

1.5 Conclusion

This report has provided a summary of security incidents to which IIJ has responded. In this report we discussed a spate of incidents related to public key certificates that took place last year, and looked at targeted attacks and their handling.

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

Authors:
Mamoru Saito
Manager of the Office of Emergency Response and Clearinghouse for Security Information, IIJ Service Division. After working in security services development for enterprise customers, Mr. Saito became the representative of the IIJ Group emergency response team, IIJ-SECT in 2001, participating in FIRST, an international group of CSIRTs. Mr. Saito serves as a steering committee member of several industry groups, including Telecom-ISAC Japan, Nippon CSIRT Association, Information Security Operation providers Group Japan, and others.

Hirohide Tsuchiya (1.2 Incident Summary)
Hirohide Tsuchiya, Hiroshi Suzuki, Tadaaki Nagao (1.3 Incident Survey)
Yuji Suga (1.4.1 Problems Related to the Issuing of Public Key Certificates)
Mamoru Saito (1.4.2 Targeted Attacks and Their Handling)
Office of Emergency Response and Clearinghouse for Security Information, IIJ Service Division

Contributors:
Masahiko Kato, Masafumi Negishi, Yasunari Momoi, Hiroaki Yoshikawa, Hiroshi Suzuki, Takahiro Haruyama, Tadashi Kobayashi, Seigo Saito
Office of Emergency Response and Clearinghouse for Security Information, IIJ Service Division

*82 For example, the Targeted Attack Countermeasure Working Group of the Information Security Operation provider Group Japan (http://www.jnsa.org/isog-j/e/index.html) is attempting to verify targeted attacks through information sharing among members. According to their interim report "NSF2012 B2 Targeted Attacks and Security Operations" (http://www.jnsa.org/seminar/nsf/2012/pro.html) (in Japanese), by sharing and examining information about targeted attacks that had occurred in the past, it was confirmed that multiple managed security service providers had observed the same type of attack. This shows that by sharing information in real-time it is possible to implement measures against certain types of targeted attack.