The Revised Unauthorized Computer Access Law

In this volume we examine the revised Unauthorized Computer Access Law, and discuss the DNS Changer malware as well as the Ghost Domain Name issue relating to DNS.

1.1 Introduction

This report summarizes incidents to which IIJ responded, based on general information obtained by IIJ itself related to the stable operation of the Internet, information from observations of incidents, information acquired through our services, and information obtained from companies and organizations with which IIJ has cooperative relationships.

This volume covers the period of time from January 1 to March 31, 2012. Following on from the previous period, with an increase in the number of smartphone users, there have been an increasing number of problems related to the handling of information on the devices and user information. Hacktivism-based attacks such as those by Anonymous also continued to occur, and the number of attacks on companies and government agencies remained at a high level.

In Middle-Eastern countries and Israel there were a series of hacking incidents and information leaks, as well as DDoS attacks on websites including critical infrastructure. Regarding vulnerabilities, an issue was discovered and fixed in multiple cache DNS server implementations including BIND.

As seen above, the Internet continues to experience many security-related incidents.

1.2 Incident Summary

Here, we discuss the IIJ handling and response to incidents that occurred between January 1 and March 31, 2012. Figure 1 shows the distribution of incidents handled during this period*1.

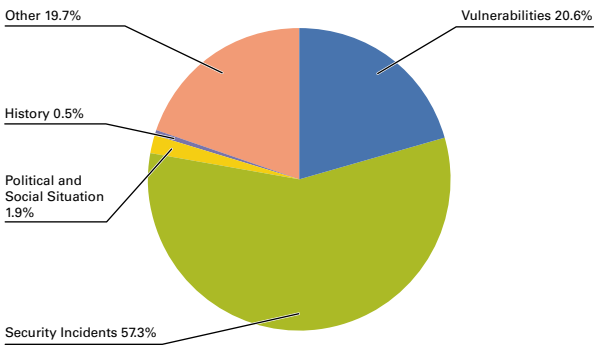


Figure 1: Incident Ratio by Category (January 1 to March 31, 2012)

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

The Activities of Anonymous and Other Hacktivists

Attacks by hacktivists such as Anonymous continued during this period. DDoS attacks and information leaks were perpetrated due to a variety of incidents and causes, targeting corporations and government-related sites in the United States and multiple countries in Europe and the Middle East. The campaign against the SOPA/PIPA bills that has been ongoing since the end of last year in the United States and the movement protesting the ACTA bill in Europe became increasingly active, with groups associated with these bills being targeted in attacks.

In January 2012 various Sony Group companies were warned they would once again be targeted in attacks in an operation called #OpSony2, following on from the attacks that took place last year. However, this attack operation did not eventuate, with the only attacks being alterations to a number of group company websites.

In February WikiLeaks announced they would release approximately 5 million internal emails from Stratfor (Strategic Forecasting Inc.) in a number of batches. The data had been provided by Anonymous, which obtained it in a hacking incident at the end of last year. Both Anonymous and WikiLeaks drew criticism for these actions.

In early March the FBI announced that they had arrested six members of LulzSec and Anonymous. One was the leader of LulzSec, who had been arrested and indicted in June of last year. It was revealed that he cooperated with the investigation after his arrest, providing the FBI with information on other LulzSec members, and attempting to dissuade Anonymous from making attacks at the FBI's behest. There were also claims that an attack would be made on the DNS root servers in late March, but no attack activity was observed, and it was confirmed that this information was false. Additionally, a group called Anonymous China launched large-scale attacks on Chinese government-related sites, which were still ongoing at the time of writing. Not much Anonymous activity had been observed in China up to this point, so we will need to keep a close watch on developments there in the coming months.

Incidents in the Middle East

Network-based attacks have occurred frequently in the Middle East in the past due to ethnic and religious conflict. During the current survey period a series of reprisal attacks were made by groups in Middle Eastern countries and Israel after credit card information was stolen from Israeli citizens by an unknown entity and posted on a message board site*2.

The attacks gradually escalated, involving the leaking of personal information such as credit card details and SNS email accounts, as well as DDoS attacks on critical infrastructure such as stock exchanges and financial institutions in Israel, Saudi Arabia and the UAE. Their websites were also hacked and information from them leaked.

Responding to Attacks on Government Institutions

Attacks targeting government institutions also continue. In February, business-related notes may have leaked from the Ministry of Agriculture, Forestry and Fisheries when they were emailed to related parties. It was announced that these notes were later used in targeted attack emails containing a virus-infected attachment that were sent to a number of personnel. At the Patent Office it was announced that internal computers had been found to be infected with a Trojan virus. In this incident, virus infections were discovered after an investigation was carried out based on information provided by the National Information Security Center, and the infected computers were later cleaned.

Among other things, the government is working to improve information security measures by checking public Web servers for vulnerabilities. At the Information Security Policy Council*3 held in January an interim report on targeted suspicious email training and an overview of the results of checking public web servers for vulnerabilities were presented.

Particular emphasis was placed on examining public-private coordination regarding information security measures against targeted attacks. This included strengthening the information security requirements demanded of suppliers for government procurement (establishment of a CSIRT within organizations, involvement of the management of the enterprise, etc.). Regarding contact and coordination between the government and companies, NISC is to promote closer ties between private

*2 Details of the attacks and the events that prompted them can be found on the following blog. Hackmageddon.com, "Middle East Cyber War Timeline Master Index" (http://hackmageddon.com/middle-east-cyber-war-timeline/).

*3 National Information Security Center, Information Security Policy Council "28th Assembly, 2012 (January 24, 2012)" (http://www.nisc.go.jp/conference/seisaku/index.html#seisaku28).

January Incidents

1 S **2nd:** The credit card information of over 400,000 Israelis were published after being stolen by an unknown entity.

2 V **4th:** A vulnerability that made brute force attacks easier was discovered in the PIN authentication specifications for Wi-Fi Protected Setup (WPS).
VU#723755 WiFi Protected Setup (WPS) PIN brute force vulnerability (http://www.kb.cert.org/vuls/id/723755) .

3 V **5th:** Multiple vulnerabilities (CVE-2012-0392 and CVE-2012-0393) including one that allowed execution of arbitrary commands were found and fixed in Apache Struts2.
"Multiple critical vulnerabilities in Struts2" (http://struts.apache.org/2.x/docs/s2-008.html).

4 V **6th:** A researcher at a U.S. security firm presented a new "Slow Read DoS" technique for attacking Web servers.
Qualys, Inc., Qualys Security Labs "Are you ready for slow reading?" (https://community.qualys.com/blogs/securitylabs/2012/01/05/slow-read).

5 S **6th:** An Australian financial institution announced they had limited connections from overseas due to DDoS attacks they experienced at the end of last year.

6 V **11th:** Microsoft published their January 2012 security bulletin, and released fixes including the MS12-004 critical update and six important updates.
"Microsoft Security Bulletin Summary for January 2012" (http://technet.microsoft.com/en-us/security/bulletin/ms12-jan).

7 V **11th:** Multiple vulnerabilities that could allow code execution were fixed in Adobe Reader and Acrobat.
"APSB12-01 Security updates available for Adobe Reader and Acrobat" (http://www.adobe.com/support/security/bulletins/apsb12-01.html).

8 V **12th:** It was revealed that the personal information of customers who had purchased Android apps using the Google Checkout service had been mistakenly disclosed to app developers, and this error was fixed.
Details regarding this incident can be found in the following Google Checkout Buyer Help article. "Internet Safety Tips"
(http://support.google.com/checkout/bin/answer.py?hl=en&hlrm=ja&answer=105821).

9 S **13th:** It was announced that the computer of an employee at the Japan Aerospace Exploration Agency had been infected with a computer virus and information on the computer leaked externally.
"Regarding the computer virus infection at JAXA" (http://www.jaxa.jp/press/2012/01/20120113_security_j.html) (in Japanese).

10 S **16th:** DDoS attacks were launched on the websites of an Israeli stock exchange and airline company.

11 S **17th:** DDoS attacks were launched on the websites of Saudi Arabian and UAE stock exchanges.

12 V **17th:** Oracle released their quarterly scheduled update, fixing a total of 78 vulnerabilities.
"Oracle Critical Patch Update Advisory - January 2012" (http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html).

13 O **18th:** Websites including Reddit, Wikipedia, and WordPress protested the SOPA/PIPA bills under discussion at the U.S. Congress by implementing measures such as site blackouts.
SOPA STRIKE, "A project of Fight for the Future" (http://sopastrike.com/).

14 O **19th:** The Japanese government announced the status of initiatives such as the implementation of sender authentication technology at government institutions and their interim report on the results of training on targeted suspicious email.
National Information Security Center, "The State of Information Security Measure Initiatives at Government Institutions"
(http://www.nisc.go.jp/active/general/torikumi.html) (in Japanese).

15 O **20th:** The "Working Group regarding the Handling of User Information via Smartphones" announced the results of a survey on the inappropriate acquisition of user information by smartphone apps.
Ministry of Internal Affairs and Communications, "Working Group regarding the Handling of User Information by Smartphones (1st)"
(http://www.soumu.go.jp/menu_sosiki/kenkyu/riyousya_ict/02kiban08_03000087.html) (in Japanese).

16 O **20th:** The Ministry of Internal Affairs and Communications and rights holder groups affiliated with the Consortium against Copyright Infringement via File-Sharing Software announced that proof-of-concept tests for changing copyright-infringing files on P2P networks into warning notices would be carried out.
Ministry of Internal Affairs and Communications, "Implementation of Proof-of-Concept Tests related to Illegal Distribution of Content via P2P File-Sharing Networks" (http://www.soumu.go.jp/menu_news/s-news/anti-pirasyefforts0123-0129.html) (in Japanese).

17 S **26th:** The Osaka prefectural police filed additional charges of creation of unauthorized commands via electromagnetic records against a man they had arrested on suspicion of sharing unauthorized commands via electromagnetic records. This was the first time that such charges for creation were laid.

18 S **26th:** Symantec released a fix for a known vulnerability affecting pcAnywhere v12.5 in response to a statement suggesting that the source code for some of their products would be leaked.
"Technical White Paper : pcAnywhere Security Recommendations"
(http://www.symantec.com/content/en/us/enterprise/white_papers/b-pcanywhere-security-recommendations-WP.pdf).

19 S **27th:** Multiple websites in Iran were altered or targeted in DDoS attacks by an unknown entity.

20 S **27th:** Malware that exploited a vulnerability already fixed by Microsoft (MS12-004) was discovered.
Trend Micro MALWARE BLOG, "Malware Leveraging MIDI Remote Code Execution Vulnerability Found"
(http://blog.trendmicro.com/malware-leveraging-midi-remote-code-execution-vulnerability-found/).

21 S **29th:** Multiple government-related sites in Japan were altered by an unknown entity.

22 O **30th:** Due to a series of attacks on the websites of government institutions, a warning was issued regarding information security measures for websites constructed or operated via outsourcing.
National Information Security Center, "Information Security Measures for Government Institution Websites that are Constructed or Operated via Outsourcing" (January 30, 2012). (http://www.nisc.go.jp/active/general/pdf/gaibuitaku_120130.pdf) (in Japanese).

23 S **31st:** An incident occurred in which sites created using WordPress were altered to redirect users to a Phoenix Exploit Kit server.
M86 Security, "Massive Compromise of WordPress-based Sites but 'Everything will be Fine'"
(http://labs.m86security.com/2012/01/massive-compromise-of-wordpress-based-sites-but-%E2%80%98everything-will-be-fine%E2%80%99/).

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

*Dates are in Japan Standard Time

associations such as MSSPs and the Nippon CSIRT Association, public security organizations, and NISC. It will also play a key role as a nexus in coordinating activities led by government ministries (the National Police Agency's Network for Sharing Cyber Intelligence Information, the Ministry of Economy, Trade and Industry's Initiative for Cyber Security Information sharing Partnership of Japan, the Ministry of Internal Affairs and Communications' Telecom-ISAC Public-Private Council, and NISC's Network for Sharing Incident Information between Ministries and Agencies).

In addition, a standard contract and provisions for enabling MSSPs to share some customer information regarding incidents with related organizations, establishment of an in-house CSIRT at companies, training for information security personnel, the convening of a symposium for public and private parties to exchange opinions, and the establishment of CSIRT at government institutions are all being considered.

Human resource development is also being examined by the "Committee for Public Awareness and Human Resource Development"*4 set up last year.

Meanwhile, a number of websites linked to government institutions were also altered during the current period, and the National Information Security Center issued a series of warnings on "Vulnerabilities Confirmed at a Number of Ministries During an Examination of Public Web Servers for Vulnerabilities," and "Security Measures for Government Institution Websites that are Constructed or Operated via Outsourcing. "The National Information Security Center also issued a "Warning regarding cases of search sites being exploited to misrepresent government sites" after incidents of users accessing or contacting fraudulent sites due to details of the intended organization not always showing in the top results at search sites. IPA has also published a report on cases in which the wrong websites are viewed via search results*5.

■ Vulnerabilities and their Handling

During this period a large number of vulnerabilities were discovered and fixed in Microsoft Windows*6*7*8*9 and applications such as Adobe Systems' Adobe Reader, Acrobat, and Flash Player, as well as Oracle's JRE. Several of these vulnerabilities were exploited before patches were released.

Regarding server applications, a quarterly update for the Oracle database server was released, fixing a number of vulnerabilities. Multiple vulnerabilities including one involving cross-site scripting were also fixed in the WordPress CMS tool. In addition to these, a patch was released for Mac OS X Lion, and several vulnerabilities in QuickTime including those that allowed arbitrary code execution were discovered and fixed. Cisco released its scheduled update, fixing multiple vulnerabilities in their router and switch firmware. A new technique for launching DoS attacks by exhausting Web server resources called "Slow Read DoS" was also released along with test tools. Additionally, an issue affecting a number of cache DNS server implementations including BIND that made it possible to keep an expired domain available*10 was disclosed. See "1.4.3 The Ghost Domain Names Vulnerability" for more information regarding this issue.

■ Smartphone Apps and the Handling of User Information

With smartphones growing in popularity, there have been an increasing number of problems related to the handling of information on the devices and user information obtained by apps.

---

*4 See the following minutes, etc. for the National Information Security Center's "Committee for Public Awareness and Human Resource Development" (http://www.nisc.go.jp/conference/seisaku/jinzai/index.html) (in Japanese). IPA and the Ministry of Economy, Trade and Industry are also carrying out initiatives related to human resource development.

*5 IPA, "Computer Virus/Unauthorized Computer Access Incident Report - January 2012 - 4. Status of Consultations Received" (http://www.ipa.go.jp/security/txt/2012/02outline.html) (in Japanese).

*6 "Microsoft Security Bulletin MS12-004 - Critical: Vulnerabilities in Windows Media Could Allow Remote Code Execution (2636391)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-004).

*7 "Microsoft Security Bulletin MS12-008 - Critical: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2660465)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-008).

*8 "Microsoft Security Bulletin MS12-016 - Critical: Vulnerabilities in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2651026)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-016).

*9 Microsoft, "Microsoft Security Bulletin MS12-020 - Critical: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-020).

*10 See the following research paper published by the discoverer for more information regarding this issue. "Ghost Domain Names: Revoked Yet Still Resolvable" (https://www.isc.org/files/imce/ghostdomain_camera.pdf).

February Incidents

1 V **1st:** Multiple vulnerabilities in Apple's Mac OS X Lion were fixed, including a QuickTime vulnerability that allowed code execution.
"About the security content of OS X Lion v10.7.3 and Security Update 2012-001" (http://support.apple.com/kb/HT5130).

2 S **2nd:** It was announced that targeted attack emails that used business notes had been sent to the Ministry of Agriculture, Forestry and Fisheries.
"Incidents of targeted attack emails at the Ministry of Agriculture, Forestry and Fisheries"
(http://www.maff.go.jp/j/press/kanbo/hyoka/120202.html) (in Japanese).

3

4 V **3rd:** A vulnerability in PHP that allowed arbitrary remote code execution was discovered and fixed.
PHP.net, "PHP 5.3.10 Released!" (http://news.php.net/php.announce/87).

5

6 S **7th:** It was announced that a number of computers at the Patent Office had been infected with a virus.
"Virus infections at the Patent Office" (http://www.meti.go.jp/press/2011/02/20120207001/20120207001.pdf) (in Japanese).

7 V **8th:** It was announced that there was an issue (CVE-2012-1033) in multiple DNS server implementations that allowed cached resource records to be extended by an external party.
US-CERT, "Vulnerability Note VU#542123 ISC BIND 9 resolver cache vulnerability" (http://www.kb.cert.org/vuls/id/542123). See the following ISC advisory for information on BIND. ISC, "Ghost Domain Names: Revoked Yet Still Resolvable"
(https://www.isc.org/software/bind/advisories/cve-2012-1033).

8

9 S **8th:** Someone claiming to be a member of Anonymous released some of the source code for Symantec's pcAnywhere.

10 S **13th:** Anonymous announced they would launch attacks on the DNS root servers in "Operation Global Blackout" on March 31. However, some questioned the reliability of this announcement, with experts pointing out that the attack would have no effect, and another Anonymous faction claimed this was a fake operation.
See the following Errata Security blog post for more information. "No, #Anonymous can't DDoS the root DNS servers"
(http://erratasec.blogspot.com.au/2012/02/no-anonymous-cant-ddos-root-dns-servers.html).

11

12

13 S **14th:** A website for the Israeli government was hacked, and information stolen from it released.

14 O **15th:** The National Information Security Center issued a warning about sites misrepresenting themselves as government sites by exploiting search sites.
"Warning regarding cases of search sites being exploited to misrepresent government sites"
(http://www.nisc.go.jp/active/general/pdf/search_kanki_120215.pdf) (in Japanese).

15 V **15th:** Multiple vulnerabilities in Oracle's JRE, including those that allowed arbitrary code execution, were discovered and fixed.
"Oracle Java SE Critical Patch Update Advisory - February 2012"
(http://www.oracle.com/technetwork/topics/security/javacpufeb2012-366318.html).

16

17 V **15th:** Microsoft published their February 2012 security bulletin, releasing four critical updates including MS12-008 and MS12-016, as well as five important updates.
"Microsoft Security Bulletin Summary for February 2012" (http://technet.microsoft.com/en-us/security/bulletin/ms12-feb).

18

19 V **15th:** Multiple vulnerabilities in Adobe Flash Player were discovered and fixed, including a cross-site scripting vulnerability that allowed fraudulent behavior by redirecting users to malicious websites.
"Security update available for Adobe Flash Player" (http://www.adobe.com/support/security/bulletins/apsb12-03.html).

20

21 S **16th:** DDoS attacks on radio stations and news sites thought to be linked to presidential elections were observed in Russia.
Arbor Networks Security Blog, "DDoS Attacks in Russia Added to Protests" (http://ddos.arbornetworks.com/2012/02/ddos-attacks-in-russia/).

22 S **18th:** It was reported that the camera system for monitoring the Russian presidential election had been targeted by DDoS attacks.

23 S **21st:** Notice was once again given that on March 8 the FBI would cease operation of the DNS servers that they had set up for victims of DNS Changer.
ISC Diary, "DNSChanger resolver shutdown deadline is March 8th" (http://isc.sans.edu/diary.html?storyid=12625).

24

25 O **22nd:** Kaspersky Lab published a report about DDoS attacks that took place in the second half of 2011.
"DDoS attacks in H2 2011" (http://www.securelist.com/en/analysis/204792221/DDoS_attacks_in_H2_2011).

26 S **23rd:** The website of a local authority and multiple related websites were targeted in DDoS attacks and alterations.

27 O **28th:** WikiLeaks began publishing Stratfor internal emails.
WikiLeaks, "The Global Intelligence Files" (http://wikileaks.org/the-gifiles.html).

28

29 O **29th:** IPA issued a "Warning regarding Vulnerabilities in Control Equipment" due to the disclosure of vulnerabilities and PoC for PLCs (Programmable Logic Controller) from a number of companies both in Japan and overseas.
"Warning regarding Vulnerabilities in Control Equipment" (http://www.ipa.go.jp/about/press/20120229.html) (in Japanese).

O **29th:** The Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry sent documents to Google requesting they provide a clear-cut explanation of the legal obligations in their new privacy policy to users.
Ministry of Internal Affairs and Communications, "Notice to Google"
(http://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000117.html) (in Japanese).

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

*Dates are in Japan Standard Time

During the period under study, an issue was identified with a number of apps for reading newspapers and magazines due to the fact that user browsing history and device identification data was being sent without permission. In one case a mechanism for obtaining information that was introduced for testing purposes had been left in an app, resulting in user information being sent despite the fact it was not received. The corresponding function was later removed.

Regarding the handling of information on smartphones, issues such as apps that request excessive privileges have been identified. The current handling of these issues is being assessed, with reports on survey results regarding the status of user information acquired from smartphones*11 being published by the "Working Group regarding the Handling of User Information by Smartphones" established under the Ministry of Internal Affairs and Communications' "Research Group for ICT Service Issues" from January. Efforts towards making smartphones safe and secure to use are also being examined, such as methods for notifying users about the handling and acquisition of user information.

The handling of user information has also caused issues in other cases, such as when it was revealed that the data of users who made purchases on the official Android Marketplace was being disclosed to creators by mistake. Furthermore, issues were identified with a function that sends information on the behavior of users to third parties that was later added to those provided by Hatena Bookmark. Critics claimed that both administrators of sites equipped with the function and users were not made sufficiently aware of it*12. GPS location information records and their inappropriate disclosure also became a topic of discussion. Unforeseen risks can occur when using information that makes it possible to determine where an individual is, like geotags attached to photos or location information apps, along with material linked to the individual such as on a blog or SNS. An article warning of these risks, "Geotagging poses security risks," has been published in the United States*13. The Tokyo Metropolitan Government has also issued a warning on the use of location information in Japan*14.

■ Security Software Source Code Leaks

During the current survey period, the source code for a security software package was leaked. In January it came to light that source code for subset of several Symantec products had been leaked*15. Symantec announced that the source code released was old, and had minimal impact on current products*16. However, it was later revealed that someone claiming to be a member of Anonymous had demanded money, and suggested that more source code would be leaked. For this reason Symantec provided new updates for some products in January*17. It is believed that this incident can be traced back to source code that was stolen in 2006.

■ DDoS Attacks

Many large-scale DDoS attacks took place during the current period. In Russia, a number of DDoS attacks were launched on radio stations and news sites in relation to the presidential elections held in March. Attacks were also made on the Web camera system used to monitor elections. In South Korea a minor launched a DDoS attack on the website of a government institution to protest government policies. Overseas customers of a securities firm in Australia were unable to participate in trading due to the firm blocking connections from overseas as a measure against the DDoS attacks they had been experiencing since the end of last year.

■ Cybercrime Initiatives

Private enterprises are moving ahead with concerted efforts to deal with cybercrime based on techniques such as botnets and phishing.

*11 Survey results were presented by Keisuke Takemori, a Senior Researcher at KDDI R&D Labs, at the 1st Working Group held on January 20, 2012. "The Sending of User Information from Smartphones" (http://www.soumu.go.jp/main_content/000143966.pdf) (in Japanese).

*12 Regarding this issue, the suspension of the function was announced in the following Hatena Bookmark Diary post. "The Hatena Bookmark Button has ceased sending behavior information obtained to third parties" (http://hatena.g.hatena.ne.jp/hatenabookmark/20120313/1331629463) (in Japanese).

*13 UNITED STATES ARMY, "Geotagging poses security risks" (http://www.army.mil/article/75165/Geotagging_poses_security_risks/).

*14 Tokyo Kurashi Web, "Be aware that uploading photos taken using smartphones and similar devices to blogs may disclose your whereabouts" (http://www.shouhiseikatu.metro.tokyo.jp/sodan/kinkyu/shohi_advice.html) (in Japanese).

*15 Sophos, naked security "Symantec's Norton AntiVirus source code exposed by hackers" (http://nakedsecurity.sophos.com/2012/01/06/symantec-norton-antivirus-source-code-hackers/).

*16 Statements from Symantec can be seen in the following Facebook post. (https://www.facebook.com/Symantec/posts/10150465997682876).

*17 See the following announcement from Symantec regarding the effects of this release on their products. "Claims by Anonymous about Symantec Source Code" (http://www.symantec.com/theme.jsp?themeid=anonymous-code-claims).

March Incidents

1 **S** **1st:** Microsoft's Windows Azure was affected by outages caused by incorrect processing of leap days.
Microsoft, "Summary of Windows Azure Service Disruption on Feb 29th, 2012"
(http://blogs.msdn.com/b/windowsazure/archive/2012/03/09/summary-of-windows-azure-service-disruption-on-feb-29th-2012.aspx)

2 3 **S** **1st:** NASA published a report stating that information leaks had occurred after hacking incidents related to attacks they had experienced between 2010 and 2011.
Examination of the Agency's Information Security,
(http://oig.nasa.gov/congressional/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf).

4 **O** **1st:** Google issued a new privacy policy that combined the policies previously prescribed for each service.
Google Official Blog, "Google's new Privacy Policy" (http://googleblog.blogspot.jp/2012/02/googles-new-privacy-policy.html)

5 6 **V** **5th:** Multiple vulnerabilities (CVE-2012-0768 and CVE-2012-0769) in Adobe Flash Player were discovered and fixed, including one that allowed code execution though memory corruption.
"APSB12-05: Security update available for Adobe Flash Player" (http://www.adobe.com/support/security/bulletins/apsb12-05.html).

7 8 **S** **5th:** It was announced that GitHub had been the target of a hacking incident due to multiple issues including a mass assignment vulnerability in Rails.
GitHub Blog, "Public Key Security Vulnerability and Mitigation" (https://github.com/blog/1068-public-key-security-vulnerability-and-mitigation).

9 **S** **7th:** The U.S. federal court granted a 120 day extension of the operation of DNS servers run to accommodate victims of DNS Changer.
Trend Micro MALWARE BLOG, "Esthost Update: DNS Changer Servers Granted Extension"
(http://blog.trendmicro.com/esthost-update-dns-changer-servers-granted-extension/).

10 11 **S** **7th:** The Federal Bureau of Investigation (FBI) announced it had charged six members of Anonymous believed to have participated in LulzSec and AntiSec both in the United States and overseas.
"Six Hackers in the United States and Abroad Charged for Crimes Affecting Over One Million Victims."
(http://www.fbi.gov/newyork/press-releases/2012/six-hackers-in-the-united-states-and-abroad-charged-for-crimes-affecting-over-one-million-victims).

12 13 **V** **14th:** Microsoft published their March 2012 security bulletin, and released fixes including the MS12-020 critical update, four important updates and one warning.
"Microsoft Security Bulletin Summary for March 2012" (http://technet.microsoft.com/en-us/security/bulletin/ms12-mar).

14 **S** **15th:** Multiple websites including the Israeli Air Force site were hacked, and information stolen from them released.

15 **O** **15th:** IPA published their "Report regarding initiatives to prevent internal fraud at organizations" that summarized domestic and overseas initiatives to prevent internal fraud.
"IPA Technical Watch Report regarding 'initiatives to prevent internal fraud at organizations'"
(https://www.ipa.go.jp/about/technicalwatch/20120315.html) (in Japanese).

16 17 18 **O** **19th:** CNCERT/CC published a report stating that the majority of IP addresses associated with attacks occurring via the Internet in China in 2011 were from Japan.
CNCERT/CC, "2011年我国互联网网络安全态势综述 " (http://www.cert.org.cn/UserFiles/File/201203192011annualreport(1).pdf) (in Chinese).See the following Sophos Naked Security post for details of this incident. "CERT China claims Japan and US lead in attacks on Chinese internet sites" (http://nakedsecurity.sophos.com/2012/03/22/cert-china-claims-japan-and-us-lead-in-attacks-on-chinese-internet-sites/).

19 20 **S** **21st:** A Russian phishing fraud group was arrested through the cooperation of security firms.
Trend Micro MALWARE BLOG, "Russian CARBERP Arrests Renew Optimism on International Cybercrime Prosecutions"
(http://blog.trendmicro.com/russian-carberp-arrests-renew-optimism-on-international-cybercrime-prosecutions/).

21 22 **O** **22nd:** IPA published "10 Major Security Threats for the Year 2012: Threats Evolving and on the Rise."
"'10 Major Security Threats for the Year 2012: Threats Evolving and on the Rise' published"
(http://www.ipa.go.jp/security/vuln/10threats2012.html) (in Japanese).

23 24 **S** **24th:** The "ZeuS" botnet was exposed through a collaboration between Microsoft's Digital Crimes Unit and members of the financial services industry.
The "ZeuS" botnet was exposed through a collaboration between Microsoft's Digital Crimes Unit and members of the financial services industry. See the following Microsoft blog post for more details. The Official Microsoft Blog, Microsoft and Financial Services Industry Leaders Target Cybercriminal Operations from Zeus Botnets
(http://blogs.technet.com/b/microsoft_blog/archive/2012/03/25/microsoft-and-financial-services-industry-leaders-target-cybercriminal-operations-

25 26 **V** **28th:** Multiple vulnerabilities (CVE-2012-0772 and CVE-2012-0773) that allowed arbitrary code execution due to memory leaks in Adobe Flash Player were discovered and fixed.
"APSB12-07: Security update available for Adobe Flash Player" (http://www.adobe.com/support/security/bulletins/apsb12-07.html).

27 28 **V** **29th:** A Cisco Security Advisory was released, fixing 13 vulnerabilities.
"Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication"
(http://www.cisco.com/cisco/web/support/JP/111/1110/1110698_Cisco_ERP_mar12-j.html).

29 30 **O** **30th:** The "Bill for Partial Revision of the Act on the Prohibition of Unauthorized Computer Access" was passed, introducing penalties for phishing among other things.
National Police Agency, "180th Session of the National Diet (ordinary session) Sponsored Bill, 'Bill for Partial Revision of the Act on the Prohibition of Unauthorized Computer Access'" (http://www.npa.go.jp/syokanhourei/kokkai/index.htm) (in Japanese).

31 **S** **31st:** The date Anonymous had announced they intended to launch Operation Global Blackout. No attacks were actually made on the DNS root servers.

S **31st:** Anonymous China hacked a number of sites in China.

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

*Dates are in Japan Standard Time

During the current survey period it was announced that Microsoft's Digital Crimes Unit had teamed up with financial institutions and investigative organizations to expose the C&C servers for the ZeuS botnet. This Microsoft group has also contributed to tracking down botnets in the past, including participation in the takedown of the Waldac botnet in February 2010 by freezing the domain used*18, and the takedown of the C&C servers for the Rustock botnet in March 2011*19. Trend Micro also announced it had worked with U.S. universities and Russian law enforcement in the arrest of a group that was carrying out phishing fraud.

In November 2011 the U.S. federal court approved a 120 day extension on operation of legitimate DNS servers initially scheduled for shut down on March 8, which had been set up to help users infected with the DNS Changer malware after the FBI seized its C&C servers and malicious DNS servers. This was due to the fact that a large number of victims were still infected. See "1.4.2 DNS Changer Malware" for more information about this issue.

This demonstrates that initiatives against cybercrime through collaboration between private companies and law enforcement are producing results. However, it is clear there are still issues, such as the amount of time it takes to provide support to victims by notifying them of infections, etc.

■ Other Trends

In other trends, due to the disclosure of multiple vulnerabilities in PLC (Programmable Logic Controller) from a number of companies*20, IPA issued a "Warning regarding Vulnerabilities in Control Equipment" that prompted the evaluation and implementation of appropriate measures for this control equipment.

The sharp rise in mobile communications traffic due to the proliferation of mobile devices such as smartphones has led to moves to improve infrastructure like public access wireless LAN networks. However, this expansion has uncovered issues such as the signal interference caused by the emergence of a variety of competing standards, as well as spoofing and information theft caused by the misuse of wireless LANs. Consequently, the Ministry of Internal Affairs and Communications established a "Study Group for Wireless LAN Business"*21 to coordinate the current status of wireless LAN, and evaluate necessary measures by identifying and organizing issues regarding safe and secure use and popularization.

Information security incidents caused by internal fraud continue to occur, and work is proceeding on a number of initiatives to prevent these kinds of incidents before they happen. IPA has published a "Report regarding initiatives to prevent internal fraud at organizations" that discusses the status of initiatives being implemented both in Japan and overseas to prevent internal fraud*22. IPA also issued "10 Major Security Threats for the Year of 2012: Threats Evolving and on the Rise," which discusses the security incidents and accidents that occurred during 2011 using case studies.

*18 Microsoft on the Issues, "Cracking Down on Botnets" (http://blogs.technet.com/b/microsoft_on_the_issues/archive/2010/02/24/cracking-down-on-botnets.aspx).

*19 Microsoft on the Issues, "Taking Down Botnets: Microsoft and the Rustock Botnet" (http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/03/17/taking-down-botnets-microsoft-and-the-rustock-botnet.aspx).

*20 ICS-CERT, "ICS-ALERT-12-020-01-S4 DISCLOSURE OF MULTIPLE PLC VULNERABILITIES IN MAJOR ICS VENDORS" (http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-020-01.pdf).

*21 Ministry of Internal Affairs and Communications, Study Group for Wireless LAN Business (http://www.soumu.go.jp/main_sosiki/kenkyu/lan/index.html) (in Japanese).

*22 IPA, "Report regarding 'initiatives to prevent internal fraud at organizations'" (http://www.ipa.go.jp/about/technicalwatch/20120315.html) (in Japanese).

1.3 Incident Survey

1.3.1 DDoS Attacks

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

■ Direct Observations

Figure 2 shows the circumstances of DDoS attacks handled by the IIJ DDoS Defense Service between January 1 and March 31, 2012. This information shows traffic anomalies judged to be attacks based on IIJ DDoS Defense Service standards. IIJ also responds to other DDoS attacks, but these incidents are excluded from the figure due to the difficulty in accurately ascertaining the facts of each situation.

There are many methods that can be used to carry out a DDoS attack, and the capacity of the environment attacked (bandwidth and server performance) will largely determine the degree of impact. Figure 2 categorizes DDoS attacks into three types: attacks on bandwidth capacity*23, attacks on servers*24, and compound attacks (several types of attacks on a single target conducted at the same time).

During the three months under study, IIJ dealt with 404 DDoS attacks. This averages to 4.4 attacks per day, indicating a decrease in the average daily number of attacks compared to our prior report. Bandwidth capacity attacks accounted for 0.2% of all incidents, server attacks accounted for 59.7%, and compound attacks accounted for the remaining 40.1%.

The largest attack observed during the period under study was classified as a compound attack, and resulted in 673Mbps of bandwidth using up to 62,000pps packets. Of all attacks, 82.4% ended within 30 minutes of commencement, 17.6% lasted between 30 minutes and 24 hours, and none lasted over 24 hours. The longest sustained attack was a compound attack that lasted for four hours and 55 minutes.

During the current survey period sustained attacks of over 1Gbps were made on services other than the IIJ DDoS Defense Service, with multiple large-scale attacks including one of up to 4Gbps and 750,000pps, and another of over 3Gbps and 1,100,000pps.

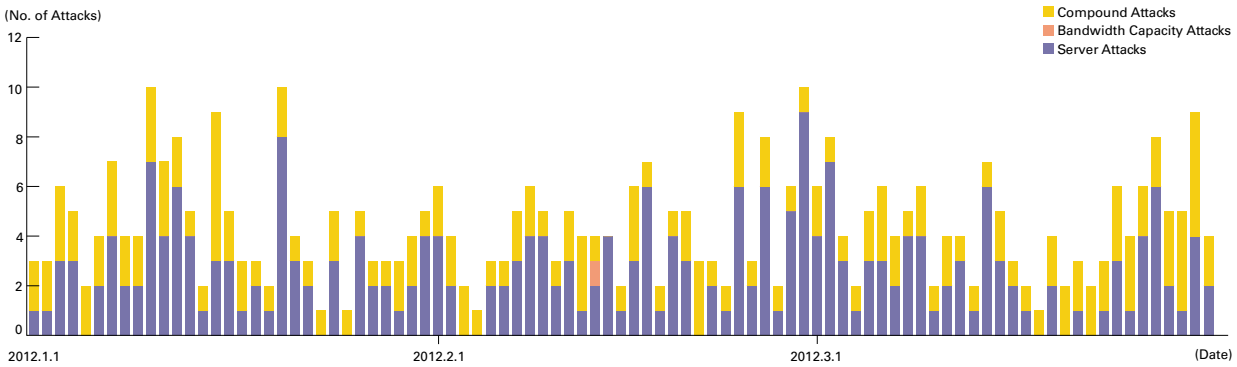


Figure 2: Trends in DDoS Attacks

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

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

In most cases, we observed an extremely large number of IP addresses, whether domestic or foreign. We believe this is accounted for by the use of IP spoofing*25 and botnet*26 usage as the method for conducting DDoS attacks.

Backscatter Observations

Next we present our observations of DDoS attack backscatter using the honeypots*27 set up by the MITF, a malware activity observation project operated by IIJ*28. By monitoring backscatter it is possible to detect some of the DDoS attacks occurring on external networks as a third party without any interposition.

For the backscatter observed between January 1 and March 31, 2012, Figure 3 shows the sender's IP addresses classified by country, and Figure 4 shows trends in packet numbers by port. The port most commonly targeted by the DDoS attacks observed was the 80/TCP port used for Web services, accounting for 60.5% 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 3306/TCP used by MySQL were also observed. Looking at the origin of backscatter thought to indicate IP addresses targeted by DDoS attacks by country in Figure 3, the United States and China accounted for large proportions at 35.7% and 26.1%, 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 hosting provider in the United States between January 4 and 5. An attack on 7208/TCP targeting a server in China was observed on January 9. An attack on a Canadian domain registry DNS server (53/TCP) was also observed on the same day.

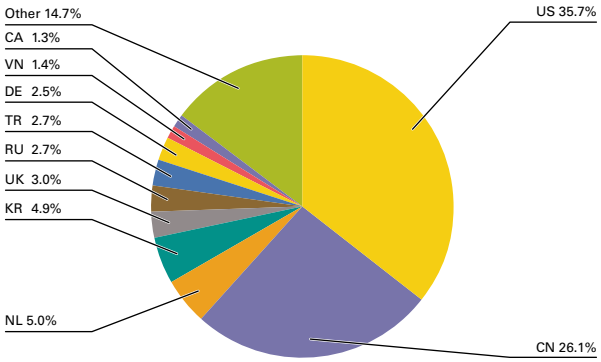


Figure 3: Distribution of DDoS Attack Targets According to Backscatter Observations (by Country, Entire Period under Study)

On February 1 many attacks on Web servers (80/TCP) thought to be made against service providers in the United States were observed. On February 22 attacks were observed on multiple Web servers in Brazil and China. One of those made on a Web server in China targeted a local search engine. This site was attacked intermittently throughout this period, but a particularly large number of attacks were observed on this day. Many attacks on MySQL (3306/TCP) were also observed between February 22 and 23 targeting a video streaming site in Turkey. On March 13 attacks on the Web servers (80/TCP) of a hosting provider in the United States were observed.

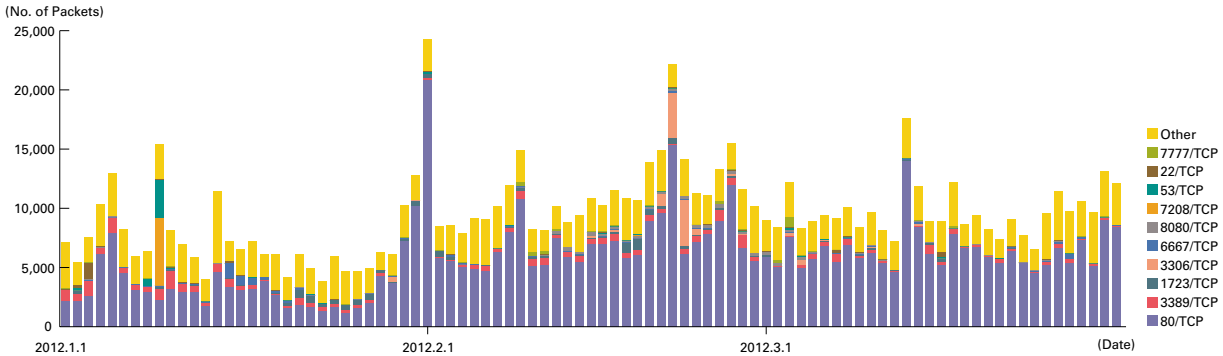


Figure 4: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)

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

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

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

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

Notable DDoS attacks during the current survey period that were detected via IIJ's observations of backscatter included attacks on the United States Department of Justice in late January thought to have been made by Anonymous. In February attacks thought to be the work of Anonymous Brasil were also detected on a number of Brazilian banks, and attacks on the Swedish government likely to have been made by Anonymous Sweden were also observed in the same month. Attacks also took place on Russian news sites in February.

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the MITF*29, a malware activity observation project operated by IIJ. The MITF uses honeypots*30 connected to the Internet in a manner similar to general users in order to observe communications arriving over the Internet. Most appear to be communications by malware selecting a target at random, or scans attempting to locate a target for attack.

■ Status of Random Communications

Figure 5 shows the distribution of sender's IP addresses by country for communications coming into the honeypots between January 1 and March 31, 2012. Figure 6 shows trends in the total volumes (incoming packets). The MITF has set up numerous honeypots for the purpose of observation. We have taken the average per honeypot, showing the trends for incoming packet types (top ten) over the entire period subject to study. Additionally, in these observations we corrected data to count multiple TCP connections as a single attack when the attack involved multiple connections to a specific port, such as attacks on MSRPC.

Much of the communications arriving at the honeypots demonstrated scanning behavior targeting TCP ports utilized by Microsoft operating systems. We also observed 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, 23/TCP used for telnet, and 3306/TCP used for MySQL. Additionally, communications of an unknown purpose were observed on ports not used by common applications, such as 2582/TCP. Looking at the overall sender distribution by country in Figure 5, we see that attacks sourced to China at 42.1%, the United States at 6.7%, and Japan and Taiwan at 6.2% were comparatively higher than the rest.

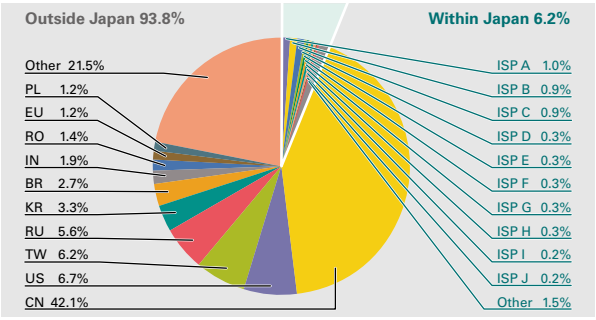


Figure 5: Sender Distribution (by Country, Entire Period under Study)

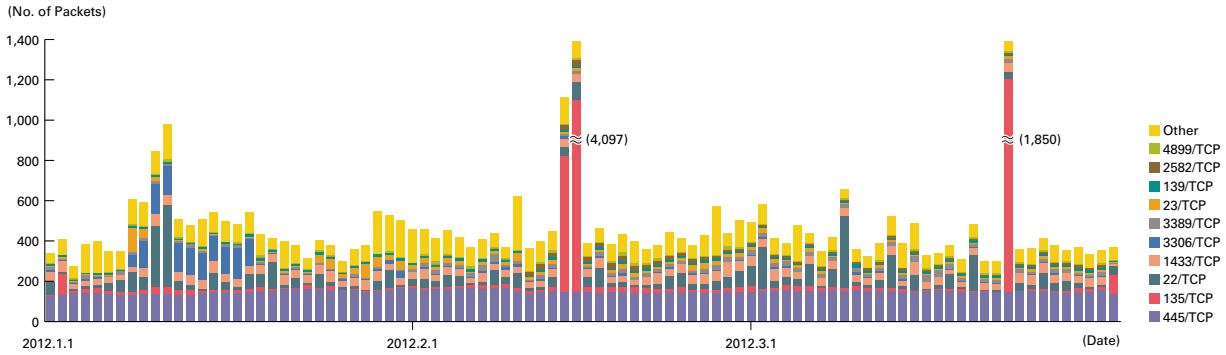


Figure 6: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

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

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

During the period under study, 135/TCP activity soared between February 14 and February 15 and on March 23, as did 3306/TCP activity between January 8 and January 18. Each of these was traced to high volumes of communications from a single IP address allocated to China.

Communications thought to be SSH dictionary attacks also occurred intermittently. For example, concentrated communications was observed coming from IP addresses in China on January 10, the United States on January 11, and India on March 9.

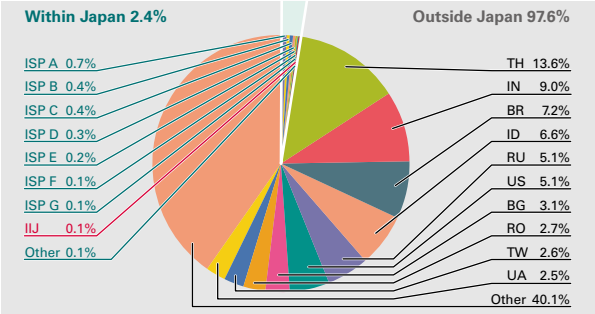


Figure 7: Distribution of Acquired Specimens by Source (by Country, Entire Period under Study, Excluding Conficker)

Malware Network Activity

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

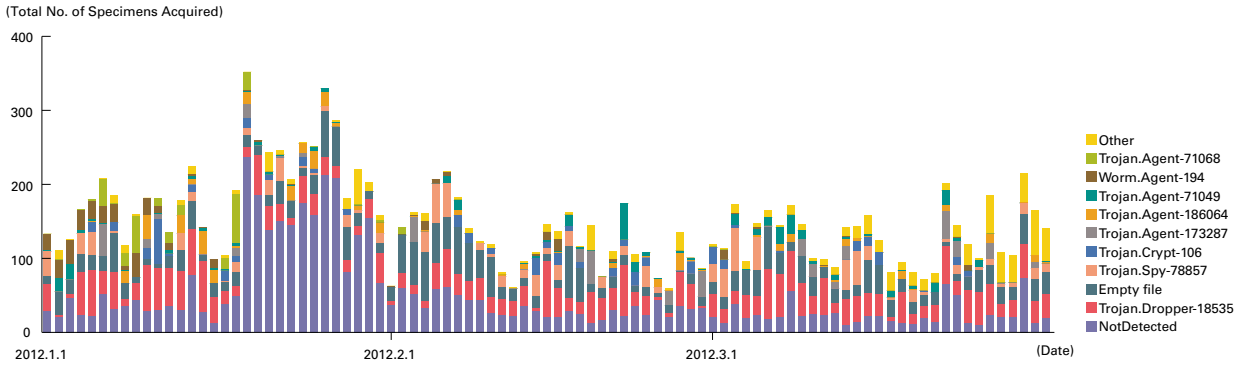


Figure 8: Trends in the Total Number of Malware Specimens Acquired (Excluding Conficker)

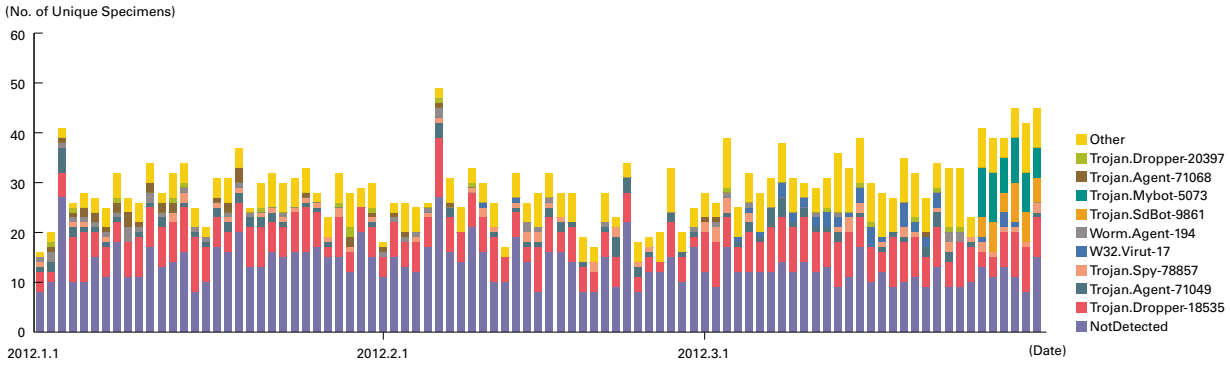


Figure 9: Trends in the Number of Malware Specimens Acquired (No. of Unique Specimens, Excluding Conficker)

*31 This indicates the malware acquired by honeypots.

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

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

On average, 150 specimens were acquired per day during the period under study, representing 29 different malware. The total number of specimens acquired has almost halved since the last report. This is due to a dramatic decrease in the number of specimens acquired from Thailand and Indonesia, which were in circulation throughout most of the previous survey period. However, between January 19 and January 30 there was in increase in the ratio of unknown specimens acquired from these two countries. After investigating more closely, we learned that two types of bots*33*34 controlled by IRC servers had been active.

Under the MITF's independent analysis, during the current period under observation 65.0% of malware specimens acquired were worms, 31.7% were bots, and 3.3% were downloaders. In addition, the MITF confirmed the presence of 20 botnet C&C servers*35 and 7 malware distribution sites.

■ MS12-020 and RDP (3389/TCP)

Microsoft published a Security Bulletin Summary*36 in March 2012. The MS12-020*37 vulnerability within this summary was mentioned in the IIJ-SECT Security Diary blog*38 due to the possibility that it could allow execution of arbitrary code without authorization from a network. Figure 10 shows the distribution of sender's IP addresses by country for communications coming into our honeypots. After a patch was released on March 14, although a slight increase was observed between March 15 and March 17, there was no significant change up to the time of writing (April 2012). Additionally, IIJ has not observed any worms or exploit code that exploits this vulnerability to execute arbitrary code. However, because those who have not applied the patch and have RDP enabled are still at risk of exploitation, we believe it is necessary to continue to keep a watchful eye on these communications.

■ Observation Status and the Conficker Worm

Including Conficker, an average of 48,358 specimens were acquired per day during the period under study, representing 1,111 different malware. These figures are 97.4% and 98.7% of those from the previous survey, representing a slight drop. Conficker remains the dominant form of malware as of this report, accounting for 99.7% of the total number of specimens acquired, and 97.3% of unique specimens. We noted fluctuations in the previous report, and since then numbers have continued to rise and fall in short cycles. Compared to IIR Vol.12 (April to June 2011) when we switched the honeypots used, the number of specimens acquired has fallen by about 17% for each category. However, as it remains the most prevalent malware by far, we will omit figures including the Conficker worm from this report onward.

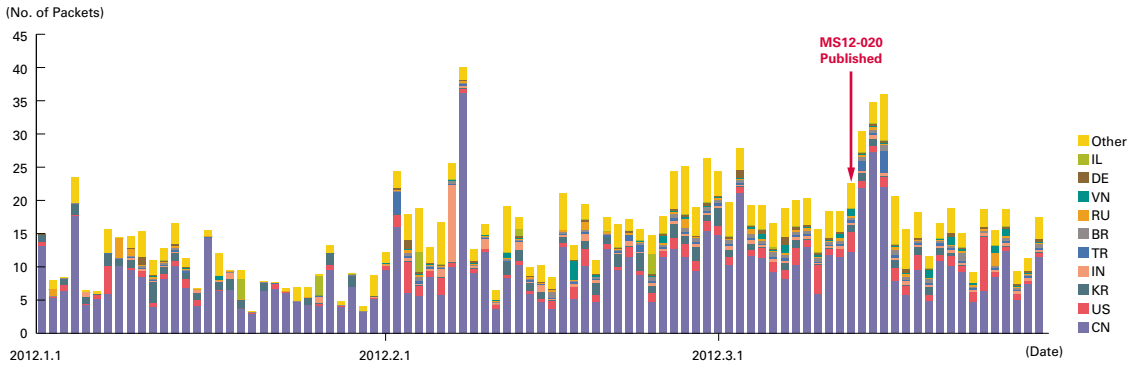


Figure 10: Communications Arriving at Honeypots (by Date, RDP (3389/TCP), per Honeypot)

*33 Trojan: Win32/Ircbrute (http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?name=Trojan%3AWin32%2FIrcbrute).
*34 Win32/Hamweq (http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fHamweq).
*35 An abbreviation of "Command & Control." A server that provides commands to a botnet consisting of a large number of bots.
*36 Microsoft, "Microsoft Security Bulletin Summary for March 2012" (http://technet.microsoft.com/en-us/security/bulletin/ms12-mar).
*37 Microsoft, "Microsoft Security Bulletin MS12-020 - Critical: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-020).
*38 IIJ-SECT Security Diary, "Warning Regarding MS12-020 Vulnerabilities" (https://sect.iij.ad.jp/d/2012/03/226127.html) (in Japanese).

1.3.3 SQL Injection Attacks

Of the types of different Web server attacks, IIJ conducts ongoing surveys related to SQL injection attacks*39. 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 11 shows the distribution of SQL injection attacks against Web servers detected between January 1 and March 31, 2012. Figure 12 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 54.2% of attacks observed, while the United States and Hong Kong accounted for 4.0% and 3.4%, 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 period under study, attacks occurring on January 20 included those from specific attack sources in the United States and Japan directed at separate specific targets. Attacks occurring on March 9 were also from a specific attack source in Hong Kong directed at another specific target. All of these attacks are thought to have been attempts to find vulnerabilities on a Web server.

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

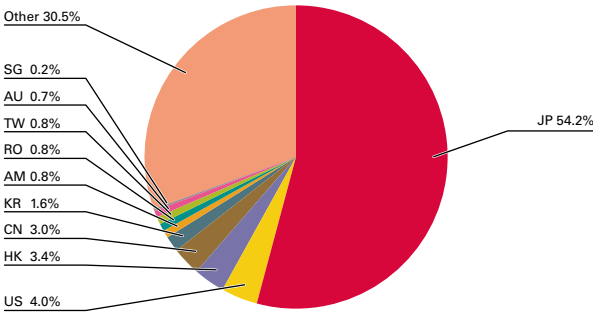


Figure 11: Distribution of SQL Injection Attacks by Source

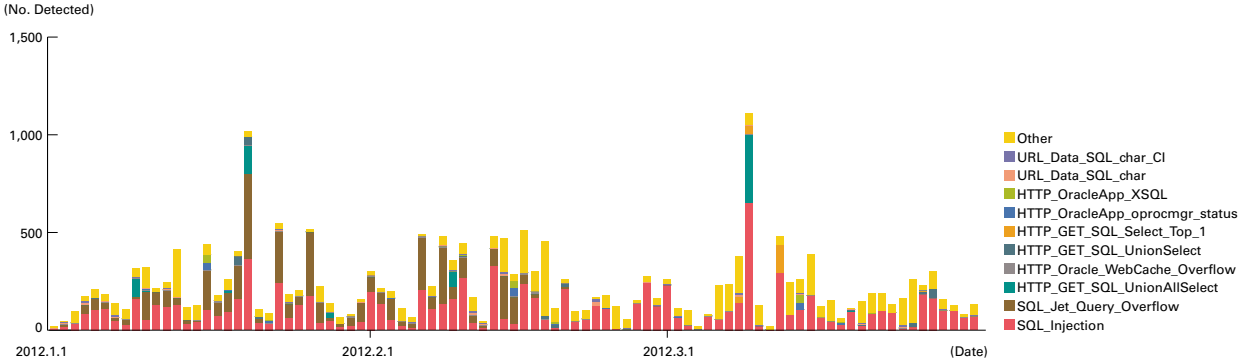


Figure 12: Trends in SQL Injection Attacks (by Day, by Attack Type)

*39 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, including discussion of revisions to Japan's Act on the Prohibition of Unauthorized Computer Access, analysis of the DNS Changer malware that can change the DNS settings referenced by users, and an explanation of the Ghost Domain Name issue reported as a DNS server vulnerability.

1.4.1 Revisions to Unauthorized Computer Access Law

On March 31, 2012, a revised version of the "Act on the Prohibition of Unauthorized Computer Access" (henceforth "Unauthorized Computer Access Law") was issued. Here we explain what led to the revisions, as well as the main revised points.

■ Global Internet-Related Issues and Legislation in Japan

With use of the Internet as an infrastructure for socioeconomic activity progressing, fraudulent behavior exploiting the Internet is increasing throughout the world*40. Because a concerted global effort is required to clamp down on fraudulent activity occurring in cyber space on a transnational scale, the Council of Europe led moves to create the "Convention on Cybercrime"*41. This convention prescribes the criminalization of unauthorized computer access, criminal procedures for data preservation, and international cooperation for the extradition of criminals. Japan signed the convention in 2001. With fraudulent activity using the Internet also occurring in Japan, a variety of legislation has been introduced here (Table 1). Major cybercrime-related laws include the following.

- **Enforcement of the Act on Regulation of Transmission of Specified Electronic Mail**
  With the popularization of mobile phones there was a dramatic increase in the volume of spam sent, and issues such as the load on communications equipment due to delivery of large volumes of mail to unknown addresses and the extortionate billing of users came to the fore. As a result this act was put into effect in July 2002, defining regulations and penalties regarding the sending of specified electronic mail such as advertisements. Since then the act has continued to be revised in response to changes in the methods used to send spam.
- **Revision of the Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children (Child Pornography Prevention Act)*42**
  This act was introduced in November 1999 to defend the rights of children. Initially the recording media for child pornography were defined as photos and video tapes, but a revision in 2004 widened this definition to include electronic records, making the publishing of child pornography on Internet sites illegal. Today, the blocking of child pornography content by Japanese ISPs has also been implemented as a stopgap measure for preventing its distribution*43.
- **Partial Revision of the Copyright Act**
  The Copyright Act was partially revised in January 2010 in response to an increase in copyright infringement, such as the sale of pirated content in Internet auctions and the distribution of illegally copied content over file-sharing software. The revisions made it illegal to knowingly sell pirated content in Internet auctions or intentionally download copyright infringing content. Since the revised act was introduced, the use of file-sharing software has been on the decline*44.
- **Partial Revision of the Penal Code**
  The "Crimes Related to Unauthorized Commands via Electromagnetic Records (Virus Crimes)" provision was added to the penal code in July 2011. Computer viruses are one of the main methods used to commit cybercrime. However, the creation and storage of computer viruses was not defined as a crime under the previous code, making it difficult to regulate. Viruses have also been created in Japan, including the Yamada virus*45 and Harada virus*46 that spread

*40 For example, in the United States the Internet Crime Complaint Center has published statistical information (http://www.ic3.gov/media/annualreports.aspx). In Japan statistical information has been published by the National Police Agency (http://www.npa.go.jp/cyber/statics/index.html) (in Japanese).
*41 The Ministry of Foreign Affairs has published information about the Convention in Japanese (http://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html) (in Japanese). See the following site for the original English (http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm).
*42 This law can be viewed using the following legal data service system (http://law.e-gov.go.jp/htmldata/H11/H11HO052.html) (in Japanese).
*43 More information regarding these initiatives can be found in Vol.12 of this report under "Internet Topics: The Blocking of Child Pornography by ISPs in Japan" (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol12_EN.pdf).
*44 The Association of Copyright for Computer Software publishes statistical information in their "Survey on the State of File-Sharing Software Usage" (http://www2.accsjp.or.jp/research/) (in Japanese).
*45 A Trojan virus that spread over file-sharing networks (http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=TROJ_MELLPON.A).
*46 A virus that spread over file-sharing networks. IPA also issued a warning at the time. "Computer Virus/Unauthorized Computer Access Incident Report - January 2008 -" (http://www.ipa.go.jp/security/txt/2008/02outline.html) (in Japanese).

Table 1: Trends in Internet-related Incidents and Legislation in Japan

Month/Year	Event in Japan	Type
April 1999	**The "Act on Control and Improvement of Amusement Business, etc." was revised.** The distribution of pornographic images over the Internet became subject to notification.	Legislation
February 2000	**The "Act on the Prohibition of Unauthorized Computer Access" came into effect.** Among other things, this made committing or aiding unauthorized computer access illegal, and made safeguards compulsory.	Legislation
November 2001	**The "Convention of Cybercrime" was established.** Each signatory country agreed to step up efforts to counter cybercrime.	Legislation
November 2001	Distribution of illegal content using WinMX became eligible for criminal punishment for the first time.	Copyright-related
November 2001	Seeing a rapid increase in spam, the Ministry of Internal Affairs and Communications established the "Unsolicited Mail Measure Research Society."	Spam
July 2002	**The "Act on Regulation of Transmission of Specified Electronic Mail" came into effect.** Regulations on the sending of spam began.	Legislation
November 2003	Arrests were made for the distribution of illegal content using the Winny P2P file-sharing software created in Japan.	Copyright-related
January 2004	**The "Unfair Competition Prevention Act" was revised.** The penal protection of trade secrets was enhanced.	Legislation
March 2004	The website for the Association of Copyright for Computer Software (ACCS) was targeted in a DDoS attack instigated by the Antinny virus that spread exclusively via Winny file-sharing networks. Later there were a large number of information leaks from Winny users infected by this virus.	Malware High volume communications Information leak
April 2004	Telecom-ISAC Japan began attempts to counter the DDoS attack on ACCS caused by the Antinny virus.	High volume communications
May 2004	The creator of Winny was arrested on suspicion of aiding and abetting copyright infringement (he was found not guilty in 2011).	Copyright-related
June 2004	**The "Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children" was revised.** Electromagnetic records became subject to the Act, and the distribution of child pornography on the Internet as well as the creation of child pornography for supply were prohibited.	Legislation
July 2004	The "Standards for Handling Software Vulnerability Information" regarding the disclosure of information on vulnerabilities were announced, and the "Information Security Early Warning Partnership" was started by IPA and JPCERT/CC as a framework for distributing vulnerability information.	Vulnerability countermeasures
November 2004	Phishing emails disguised as being from major credit card companies and portal sites were sent out.	Phishing
December 2004	The Ministry of Economy, Trade and Industry established the "Anti-Phishing Email Conference."	Phishing
April 2005	The Anti-Phishing Working Group was established.	Phishing
April 2005	**The "Personal Information Protection Law" came into effect.** This defined business operators handling personal information and determined their obligations, while also defining penalties for infringement.	Legislation
February 2006	Telecom-ISAC Japan cooperated with ISP member companies to begin sending warnings via email to users infected with Antinny, which was attacking the ACCS website.	Malware
March 2006	With information leaks due to the use of file-sharing software occurring frequently, the Chief Cabinet Secretary called on citizens to stop using Winny.	Information leak
November 2006	Due to the use of file-sharing software taking up a noticeable portion of communications bandwidth, the Ministry of Internal Affairs and Communications put in place a "Conference on Network Neutrality."	Bandwidth control
November 2006	The Ministry of Internal Affairs and Communications announced that in their view spam countermeasures such as OP25B and sender authentication used by ISPs were valid business practices.	Spam
May 2007	Three people were arrested for the distribution of illegal content using Winny. More arrests followed.	Copyright-related
September 2007	Four telecommunications industry associations established the "Working Group for Discussing Guidelines regarding Operational Standards for Bandwidth Control."	Bandwidth control
January 2008	The creator of a virus circulating on Winny (a variant of the Harada virus) was arrested for copyright infringement.	Malware
March 2008	The National Police Agency made an announcement on "Issues regarding copyright infringement using file-sharing software such as Winny and their countermeasures."	Copyright-related
May 2008	"Guidelines regarding Operational Standards for Bandwidth Control" were published as standards for bandwidth control based on the volume of communications utilized.	Bandwidth control
March 2009	The National Police Agency made an announcement on "Issues regarding the distribution of child pornography on the Internet and their countermeasures."	Child pornography
January 2010	**The "Copyright Act" was revised.** The downloading of copyright infringing content distributed illegally using file-sharing software such as Winny was prohibited.	Legislation
August 2010	The Ika-Tako virus spread, and the creator was arrested.	Malware
March 2011	The Internet Content Safety Association was established. In April of the same year the blocking of child pornography on the Internet began.	Child pornography
April 2011	The National Police Agency made an announcement on "Measures for achieving a safe, secure, and responsible community of cyber citizens."	Unauthorized access
June 2011	A committee for aggregating public-private opinions on measures for preventing unauthorized access (public-private board) was put in place.	Unauthorized access
July 2011	**The "Penal Code" was revised.** An article on Crimes Related to Unauthorized Commands via Electromagnetic Records (Virus Crimes) was added. The creation, supply, and storage of computer viruses was prohibited.	Legislation
August 2011	The National Police Agency set up "Countermeasures against espionage activities in cyberspace (cyber-intelligence)."	Malware Targeted attacks
September 2011	Targeted attacks were made on major corporations and government agencies.	Targeted attacks
October 2011	The Ministry of Economy, Trade and Industry led the establishment of the "Initiative for Cyber Security Information sharing Partnership of Japan."	Unauthorized access
May 2012	**The "Act on the Prohibition of Unauthorized Computer Access" was revised.** The set up of phishing sites and procurement and storage of IDs/passwords by unauthorized means were prohibited.	Legislation

mainly via users of file-sharing software. In the Ika-Tako virus incident*47, the creator was actually arrested for copyright infringement and defamation of character. After the subsequent revisions to the code, the creation and storage of these computer viruses became illegal.

In addition to these laws, the Unauthorized Computer Access Law was also revised due to the need to respond to new kinds of fraudulent activity. We provide an overview of the changes later in this section.

■ The Unauthorized Computer Access Law

The "Unauthorized Computer Access Law" that has undergone revision was first enacted in February 2000, with the aim of preventing high-tech crimes and preserving the integrity of electronic communications. Its two main provisions relate to prohibiting unauthorized access and supporting protective measures. Unauthorized access as presented here can be regarded as circumventing the identification codes (IDs and passwords) protecting an electronic computer to use it without consent. This mainly covers behavior such as the misuse of another individual's identification codes (ID and password) without consent or the hacking of a computer by attacking a system's vulnerability over the Internet.

■ Events Leading up to the Revisions

While the Internet has become a useful tool in our daily lives, statistics showing that criminal acts are also on the rise have been published. Among these the theft of account information is most prevalent, and during 2011 the theft of account information using phishing sites and brute force and dictionary attacks on user IDs and passwords together accounted for approximately half of all techniques used for unauthorized access*48.

It has already been 10 years since the Unauthorized Computer Access Law was enacted. As can been seen from the cases presented here, the criminal techniques used are changing over time. It became clear that the previous Unauthorized Computer Access Law had limited effect, as it did not take into account new methodology such as phishing, and it only made arrest possible when attempts at unauthorized access were successful. With this in mind, future countermeasures against unauthorized access were proposed in the 2010 report, "Measures for achieving a safe, secure, and responsible community of cyber citizens"*49 at the National Police Agency's General Security Countermeasures Conference for reviewing policies. This included "basic concepts," "responding to new methodology," "improving protective measures by access administrators, etc.," and "investigating and enhancing unauthorized access countermeasures via the solicitation of public and private opinions." Taking on board these proposals the National Police Agency sought feedback from the public and private sectors, and the current revisions to the Unauthorized Computer Access Law were made.

As an example of the revisions made, the act of providing another individual's ID or password to a third party without their consent was prohibited, as was their use. Regarding protective measures and their support, legal requirements were introduced to support protective measures by access administrators and oblige administrative authorities to make efforts to perform public relations and inform the public. Other changes include stiffer statutory penalties.

■ Overview of Revised Content

The noteworthy changes made to the Unauthorized Computer Access Law are described below. In addition to prohibiting the unauthorized procurement of IDs or passwords, the creation of phishing sites, and the sending of targeted attack email, provisions regarding public-private coordination were also added.

- **Prohibition of the unauthorized acquisition of another individual's identification codes (Article 4)**
  The acquisition of another individual's identification codes (ID, password, etc.) by unauthorized means with the intent to exploit them to access a computer without authorization is now prohibited. For example, purchasing another individual's ID or password on an underground site, etc., falls under the provisions of this article.

*47 A virus created by the creator of the Harada virus. See the following Trend Micro SECURITY BLOG post for more details. "Reconfirming security measures for the year-end and New Year" (http://blog.trendmicro.co.jp/archives/3269) (in Japanese)

*48 The National Police Agency's statistics are as follows: "Publication of the Status of Unauthorized Access Incidents in 2011" (http://www.npa.go.jp/cyber/statics/h23/pdf040.pdf) (in Japanese).

*49 National Police Agency "Measures for achieving a safe, secure, and responsible community of cyber citizens" (http://www.npa.go.jp/cyber/csmeeting/h22/pdf/pdf22.pdf) (in Japanese).

- **Prohibition of the unauthorized storage of another individual's identification codes (Article 6)**
  The unauthorized storage of another individual's identification codes with the intent to exploit them to access a computer without authorization was also prohibited in these revisions. For example, storing another individual's ID or password for the purpose of selling it falls under the provisions of this article.
- **Prohibition of unauthorized requests for identification codes (Article 7)**
  Two of the most significant changes made in these revisions were criminalizing the establishment of phishing sites in item 1 of Article 7, and criminalizing the transmission of phishing emails in item 2 of Article 7. The latter provisions also apply to some targeted attack email.
- **Assistance from Prefectural Public Safety Commissions (Article 10, Paragraph 2)**
  The Unauthorized Computer Access Law had provisions regarding the dissemination of information and raising awareness before revisions were made, but these revisions added provisions regarding the supply of information to private sector trade associations, etc.

Each of the provisions stated that exceptions would be made in cases where there is no fraudulent intent despite similar activity being involved, such as security assessment providers and cache servers on the Internet. Care was taken not to obstruct activities that contribute to improving security.

■ Summary

These revisions criminalized activities such as phishing, sending targeted attack email, and selling and purchasing IDs. At the time of writing the revised Unauthorized Computer Access Law has not yet been enacted, so it is not clear how this law will be put into operation. However, with these revisions it is now possible for law enforcement to implement measures against a number of activities that previously could only be dealt with using technology. IIJ will continue to keep a close watch on future legal trends such as these, and strive to maintain a safe Internet environment through cooperation with industry associations.

1.4.2 DNS Changer Malware

DNS Changer is a variant of the malware known as TDL4 or TDSS*50. In November 2011 the C&C servers for this malware and malicious DNS servers related to it were seized by the FBI, containing its activity*51. After it was shut down, ISC operated legitimate DNS servers in place of these malicious DNS servers, allowing infected users to continue using the Internet without issue. Because these DNS servers were due to be taken offline on March 8, 2012, a warning was also issued by the IIJ-SECT Security Diary blog*52. Then, as mentioned in a subsequent announcement*53, the United States federal courts decided to extend operation of these DNS servers until July 9, 2012 (U.S. time)*54. Meanwhile, as those infected with this malware still must be dealt with, we will once again give an account of this incident and issue a reminder in this report.

■ Background to this Warning

At the time of the FBI seizure, DNS Changer had infected over 4 million computers around the world. At NANOG 54 held in February 2012, discussions took place regarding the fact that those still infected would no longer be able to use the Internet to browse the Web or send and receive email due to the legitimate DNS servers operated by ISC being taken offline on March 8. With a survey conducted by the DCWG (DNS Changer Working Group)*55 confirming that there were approximately 450,000 infected computers as of the end of January, IIJ also issued an urgent warning.

■ An Overview of DNS Changer

DNS Changer is said to have caused damages of at least 14 million dollars, and had over 100 C&C servers distributed around the world.

Other malware in the past has also exploited the name resolution system or altered how communications were displayed. For example, MyDoom interfered with the operation of anti-virus software by rewriting the hosts files, and SpyEye and ZeuS

*50 DNS Changer is also known by a variety of other names such as Ghost Click, Zlob, and Alureon.
*51 See the following URL for details regarding this operation, known as Operation Ghost Click. "Operation Ghost Click International Cyber Ring That Infected Millions of Computers Dismantled" (http://www.fbi.gov/news/stories/2011/november/malware_110911).
*52 IIJ-SECT Security Diary, "Warning Regarding DNS Changer Malware Infections" (https://sect.iij.ad.jp/d/2012/02/245395.html) (in Japanese).
*53 IIJ-SECT Security Diary, "Warning Regarding DNS Changer Malware Infections (Follow-up)" (https://sect.iij.ad.jp/d/2012/03/074130.html) (in Japanese).
*54 The fact that the DNS servers will be suspended on July 9 is mentioned in the following URL. (http://www.fbi.gov/news/stories/2011/november/malware_110911).
*55 DCWG (DNS Changer Working Group) (http://www.dcwg.org/).

obtained personal information fraudulently by inserting input fields for credit card numbers or random number tables for bank accounts on websites viewed on an infected computer when the URLs for certain financial institutions were displayed. However, DNS Changer uses the technique of redirecting communications directly to malicious servers by preparing malicious DNS servers and rewriting DNS server settings. Figure 13 shows network settings after infection with DNS Changer. You can see that the DNS server has been rewritten to the address range indicated in FBI documentation*56. This demonstrates that changes to DNS settings are not hidden from users, and can be seen when viewing a computer's settings. On first glance this does not appear to be a very clever technique, but as a large number of users remained unaware of the infection, it is fair to say that in the end this technique made a sizable impact. Another unique aspect of DNS Changer was the sheer scale of the operation, with the crime syndicate behind it operating as an IT company, and having subsidiaries registered as hosting companies and registrars*57.

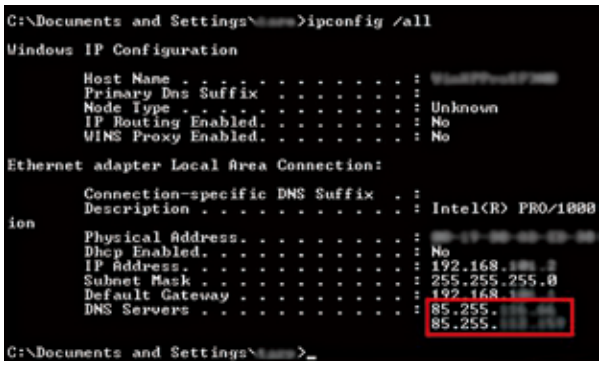
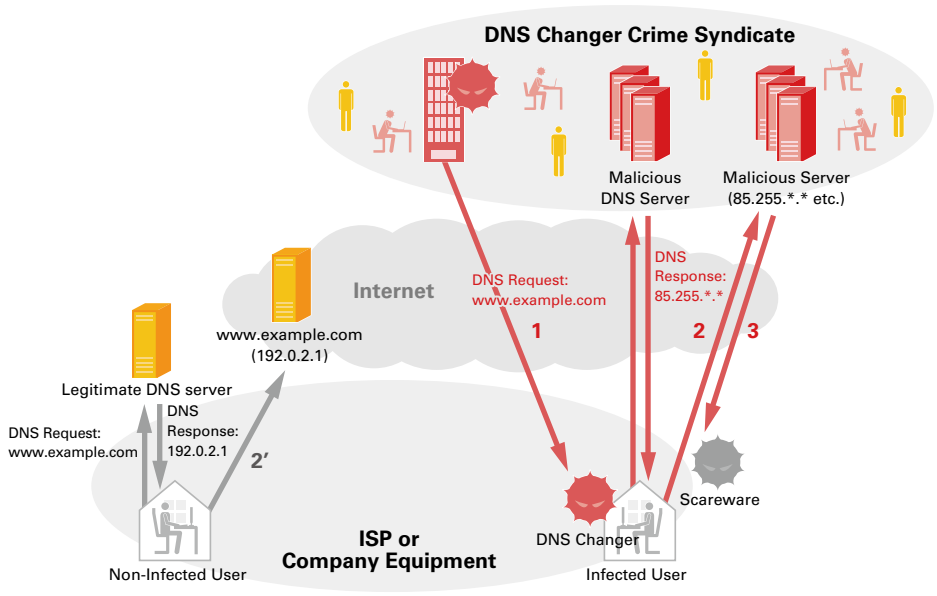


Figure 13: DNS Settings Upon DNS Changer Infection

Figure 14 gives an overview of DNS Changer. DNS Changer infections are said to have spread via drive-by downloads on websites and using social engineering by masquerading as video player software to induce users to download and execute the malware*58. Once infected, the malware rewrites DNS settings to those for an external malicious server, and attempts to defraud users of money using methods such as distorting Web search results using click-jacking, or replacing advertisements on websites viewed. For example, there have been reports of incidents such as



1. A computer is infected via social engineering (e.g. coercing a user to download a file disguised as video player software) or drive-by download, and DNS settings rewritten with malicious server details.
2. When the user accesses a certain site such as a search engine (www.example.com in this example), requests are sent to a malicious DNS server, and the user is redirected to a malicious server.

2'. Non-infected users are configured to use the DNS servers for their ISP, etc., and regular DNS responses are returned, so they are able to connect to the server they requested.

3. Users are defrauded of money through methods such as coercing them to download scareware from a malicious server.

Figure 14: DNS Changer Overview

*56 The following document describes the address range of the malicious DNS servers used by DNS Changer. "DNSChanger Malware" (http://www.fbi.gov/news/stories/2011/november/malware_110911/DNS-changer-malware.pdf).

*57 Information about this incident was posted on the Trend Micro blog site. Trend Micro MALWARE BLOG, "Esthost Taken Down - Biggest Cybercriminal Takedown in History" (http://blog.trendmicro.com/esthost-taken-down-biggest-cybercriminal-takedown-in-history/).

*58 The following FBI press release described the malware's route of infection. "Manhattan U.S. Attorney Charges Seven Individuals for Engineering Sophisticated Internet Fraud Scheme That Infected Millions of Computers Worldwide and Manipulated Internet Advertising Business" (http://www.fbi.gov/newyork/press-releases/2011/manhattan-u.s.-attorney-charges-seven-individuals-for-engineering-sophisticated-internet-fraud-scheme-that-infected-millions-of-computers-worldwide-and-manipulated-internet-advertising-business).

scareware*59 (fake anti-virus software) being installed to defraud money by replacing search results with links to malicious sites when a user performs a search on how to remove spyware*60.

■ A Wide Range of Variants

DNS Changer is itself a variant of TDL4 or TDSS, and exhibits a wide variety of behavior. Its appearance was confirmed in 2005*61, and it was active for over 6 years. In 2008 a type that attempted to hijack entire local networks by emulating a DHCP server appeared*62, and there have been reports of variants that infiltrate routers left set to their default passwords and alter their settings*63, save malicious code to the master boot record, or target Mac computers. Among the specimens that IIJ has obtained itself were those that did not rewrite DNS settings, despite the fact they were detected as DNS Changer by anti-virus software and exhibited similar behavior under IIJ analysis. These are likely to be malware with characteristics similar to DNS Changer or TDL4 or TDSS, so it is possible you will remain unaware of the fact that you have been infected if you only check the DNS settings.

■ Countermeasures

Currently it is possible to detect DNS Changer using a variety of anti-virus software*64, as its C&C servers have been seized and it is no longer able to mutate by updating itself. It is also possible to confirm infection using removal tools released by major anti-virus vendors*65.

If you are suddenly unable to view websites or send and receive email after July 9, 2012 (U.S. time), there is a good chance that your computer is infected with this malware. However, DNS settings remain in their rewritten state even after the malware is detected and removed, so it will be necessary to reconfigure DNS-related settings yourself based on the information provider by your ISP, etc. Additionally, as mentioned above some variants save malicious code to the master boot record, so even after removal the malware may be restored from that code and re-infect the computer when you reboot it. In this case, you will need to take measures such as overwriting the master boot record during restoration, or reinstalling after formatting the hard disk.

To avoid being infected with this malware, it is important to implement drive-by download countermeasures such as keeping your OS up to date with Windows Update, installing anti-virus software, always applying the latest pattern files, keeping Web browser plug-ins up to date, and deleting all unnecessary software. Measures to protect yourself from social engineering such as being wary of opening email attachments and clicking links on websites or in email are also crucial.

1.4.3 The Ghost Domain Names Vulnerability

■ About Ghost Domain Names

This vulnerability was disclosed in a research paper by Professor Haixin Duan of Tsinghua University and his colleagues called “Ghost Domain Names: Revoked Yet Still Resolvable” at the NDSS Symposium 2012*66 held on February 8, 2012. This

*59 See Vol.3 of this report under “1.4.3 Scareware” (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol03_EN.pdf) for an explanation of scareware.

*60 A demonstration of this has been published in video form on the GFI blog. “Movie Time: DNS Changer trojan” (http://www.gfi.com/blog/movie-time-dns-changer-trojan/).

*61 By checking the Trend Micro or Symantec databases we can see this malware appeared in 2005. (http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=TROJ_DNSCHANGE.A), (http://www.symantec.com/en/us/security_response/writeup.jsp?docid=2005-030413-5303-99).

*62 Variants of DNS Changer that emulate DHCP are introduced on the SANS blog ISC Diary “Rogue DHCP Servers” (http://isc.sans.edu/diary.html?storyid=5434) or Symantec site “Trojan.Flush.M” (http://www.symantec.com/security_response/writeup.jsp?docid=2008-120318-5914-99).

*63 NANOG 54 (North American Network Operators’ Group) BoF documents give examples such as UTSTARCOM, D-Link, and Linksys, but the information about the functions modifying router settings isn’t based on practical incidents or code analysis results, only going as far as saying that router settings are included in the configuration data structure of variants.

*64 However, as it is possible you may also be infected with other malware, it would be best to confirm the support status of the anti-virus software you are using prior to removal. Also, although this has not been confirmed by IIJ, it appears that some specimens interfere with the operation of anti-virus software, so it is possible the anti-virus software installed may not detect the malware.

*65 For example, Kaspersky Lab issued the following warning along with their removal tool, explaining the removal process in detail. Viruslist.com “[Warning] DNS Changer” (http://www.viruslistjp.com/analysis/?pubid=999999996) (in Japanese).

*66 19th Annual Network & Distributed System Security Symposium (http://www.isoc.org/isoc/conferences/ndss/12/).

was a new type of vulnerability that affected a large number of DNS implementations at the time of its disclosure. Details can be found in the research paper and presentation materials published on the author's website*67. JPRS has also released a commentary on this issue in Japanese*68.

On February 7, 2012, before the vulnerability was disclosed, the developer of the popular BIND DNS server software ISC released a security advisory*69, but the details of the vulnerability were not published until the presentation the following day. After the presentation on February 8, ISC launched an investigation into the impact of the vulnerability and announced they did not plan to release an emergency patch. Although a fix was not forthcoming at this stage, the vulnerability was fixed along with other bugs in the version released on April 5, 2012.

The Domain Resolution Process

DNS domains have a hierarchical structure with the root (.) at the top, and name resolution must flow from top to bottom. This requires a complicated process involving multiple queries to different servers, as well as management of their status. The default DNS clients for each OS send queries for only the target domain name to a DNS caching server, instead of following this complicated process. DNS clients that behave this way are called stub resolvers. Depending on the OS and configuration, the results obtained are also sometimes cached to improve response.

Meanwhile, DNS caching servers receive queries from stub resolvers and perform name resolution from the top-level root down to the target domain. DNS clients that behave this way are called full-service resolvers. Figure 15 shows the relationship between each type of DNS server and DNS client.

As their name suggests, cache DNS servers cache the results obtained from recursive queries as well as the outcome of this process. This is an extremely effective way to reduce the traffic of authoritative DNS servers and cache DNS servers, and also improve client responses. Additional benefits are provided when multiple users use the same cache DNS server, as the retained cache is also shared between those users so frequently accessed domains are always cached.

The valid lifespan of cache is defined as the TTL for each record. Because open values are used with authoritative DNS servers, the owner of a domain can exert some control over when the cache will expire. Based on this value cache DNS servers determine whether to use the cache already saved or treat the cache as expired and send another query.

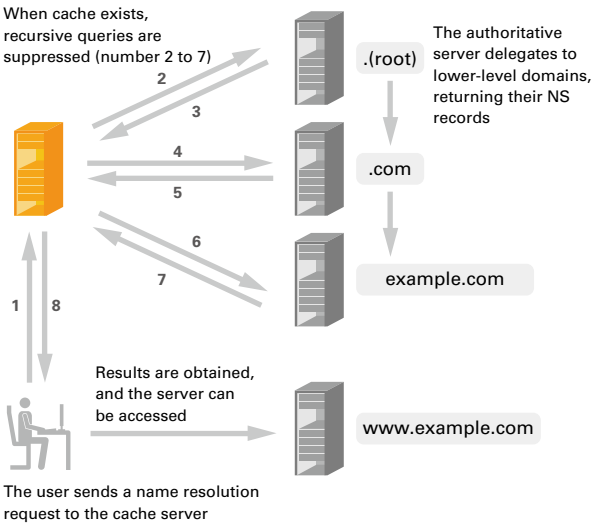


Figure 15: Standard Name Resolution Processing

The Cause of this Vulnerability

The vulnerability arises from the handling of NS records for higher and lower-level zones on cache DNS servers. Though both are NS records, their usage differs. NS records for higher levels are only used to delegate to lower-level domains, but the lower-level NS record that is delegated to holds authority.

*67 "Ghost Domain Name: Revoked Yet Still Resolvable (in NDSS 2012) "(http://netsec.ccert.edu.cn/duanhx/archives/1313).
*68 "About the ghost domain names vulnerability" (http://jprs.jp/tech/notice/2012-02-17-ghost-domain-names.html) (in Japanese).
*69 Internet Systems Consortium, "CVE-2012-1033 Ghost Domain Names: Revoked Yet Still Resolvable" (https://www.isc.org/software/bind/advisories/cve-2012-1033).

This hierarchy is specified in RFC 2181*70, but it is not explicitly stated what action to take in situations such as the one identified in this vulnerability. This means the outcome depends on the individual DNS server software implementations, and in many cases the NS record set to the lower-level zone that holds authority is given priority.

Regarding the record for the zone itself, giving the lower-level domain priority meets RFC specifications. However, as long as a valid NS record is cached, the behavior suppresses queries about delegated records dependent on the NS record, and as a result the ghost domain names vulnerability occurs.

Even if specific implementations were found to be affected by this vulnerability, this behavior would not be in violation of that specified in the RFC. However, as it has now been identified as an issue, we expect that affected implementations will be fixed in the future.

Comparison with Known Attacks

Several vulnerabilities that only affect certain DNS implementations are found each year. This is a vulnerability that impacts a large number of DNS implementations just like the one disclosed by Dan Kaminsky in July 2008.

The vulnerability disclosed by Dan Kaminsky*71 could potentially have been used in cache poisoning to enable malicious attackers to inject arbitrary records into an arbitrary domain. If such an attack was successful, users could be redirected to malicious servers even when accessing a legitimate domain. Because this affects all users of the same cache DNS server, the potential for damage is immense if a server that accommodates many users is targeted. This vulnerability received a significant amount of attention when it was disclosed due to the ease of attack and the sizable impact if such an attack was successful. DNSSEC came to the fore as a fundamental countermeasure for this vulnerability, accelerating its popularization*72.

Although the current issue also affects a large number of DNS implementations, a successful attack would not have the same impact. This new vulnerability also makes it possible to prevent the cache for a domain you own from expiring, and does not enable malicious attacks such as the cache poisoning of domains owned by others.

In most cases the owner of a domain is also responsible for its configuration, and there is no reason to prevent the cache for your own domain from expiring. The only time it would have an effect is if settings were changed against the owner's wishes.

This would apply in cases such as when a domain is seized by law enforcement. When the seizure occurs, the delegation settings for the domain are forcibly altered or revoked regardless of the domain owner's intention. Both methods effectively shut down the domain, but when a domain is seized a warning is also given to users accessing it by redirecting them to a server that explains the situation. At this point the domain owner is no longer able to change settings, and cannot restore them. DNS name resolution has a hierarchical structure, so when delegation from a higher-level domain is lost, settings made on lower-levels have no effect. This means that changing domain delegation information forcefully shuts down a domain. This is shown in Figure 16.

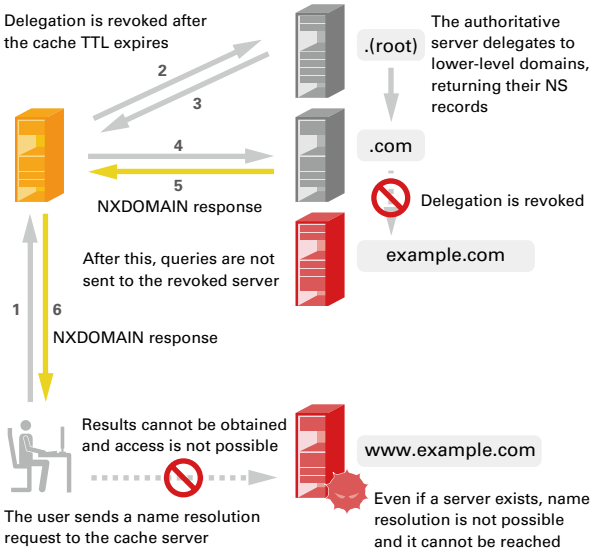


Figure 16: Name Resolution Processing when a Domain is Seized

*70 IETF, "RFC 2181 Clarifications to the DNS Specification" (http://www.ietf.org/rfc/rfc2181.txt).

*71 Introduced in Vol.2 of this report under "1.4.1 DNS Cache Poisoning" (http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol02.pdf) (in Japanese).

*72 ICANN Research, "TLD DNSSEC Report" (http://stats.research.icann.org/dns/tld_report/).

Normally a cache DNS server will obtain new delegation information from the authoritative DNS server once the TTL for the corresponding domain expires, and then delegation information on the cache DNS server will be updated. However, the owner of a seized domain can use the vulnerability identified here to maintain old delegation information without obtaining new data from the cache DNS server. This process is shown in Figure 17.

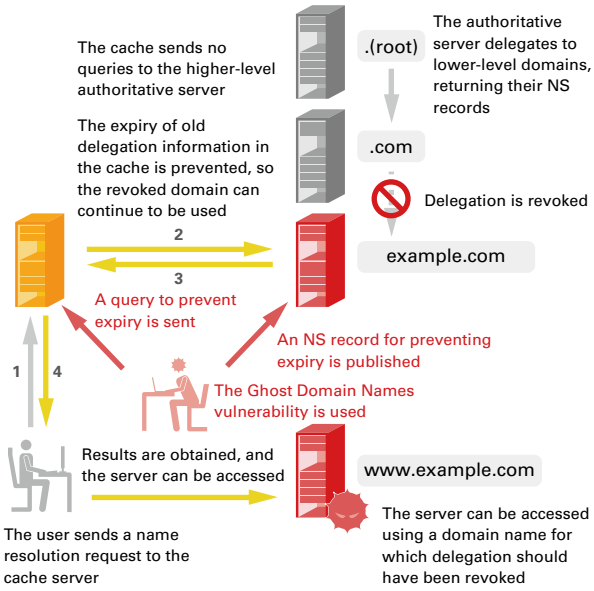


Figure 17: Name Resolution Processing when a Domain is Seized (Ghost Domain Names)

The attack method used here depends on the cache update system, and to succeed the cache DNS server must still retain delegation information from before the domain seizure in their cache. Servers launched after a domain is seized or servers that have lost their cache due to a reboot, etc., already have new delegation information in their cache, rendering attacks ineffective.

■ Summary

We believe that this incident did not cause a great stir despite affecting many DNS implementations because exploiting the vulnerability has little impact. However, when this technique is used to keep a domain that should have been deleted online, it is not possible to avoid negative impact via user systems or warnings alone. This means that even though the impact is limited, it is necessary to improve DNS implementations and operations to prevent communications not intended by users from occurring due to DNS.

1.5 Conclusion

This report has provided a summary of security incidents to which IIJ has responded. In this volume we discussed revisions to the Unauthorized Computer Access Law, and examined the DNS Changer malware that rewrites the DNS settings referenced by users, as well as the Ghost Domain Name issue reported as a DNS server vulnerability.

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 Operation 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, Masafumi Negishi (1.2 Incident Summary)
Hirohide Tsuchiya, Hiroshi Suzuki, Tadashi Kobayashi (1.3 Incident Survey)
Masahiko Kato, Mamoru Saito (1.4.1 Revisions to the Unauthorized Computer Access Law)
Hiroshi Suzuki (1.4.2 DNS Changer Malware)
Tadashi Kobayashi (1.4.3 The Ghost Domain Names Vulnerability)
Office of Emergency Response and Clearinghouse for Security Information, IIJ Service Operation Division

Contributors:
Yuji Suga, Yasunari Momoi, Hiroaki Yoshikawa, Seigo Saito, Takahiro Haruyama
Office of Emergency Response and Clearinghouse for Security Information, IIJ Service Operation Division