Forward Secrecy

In this report, we discuss points to note regarding memory forensics for devices equipped with large amounts of memory, examine the forward secrecy technology that improves the security of encrypted communications, and look at website defacement surveys carried out using Web crawlers.

1.1 Introduction

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

This volume covers the period of time from October 1 through December 31, 2013. Following on from those in the last survey period, in this period a number of hacktivism-based attacks, including some activity targeting Japan, were made by Anonymous and other groups. Attacks targeting authentication information are also continuing to occur, including an incident overseas in which tens of millions of user IDs and passwords were leaked. In relation to this, list-based attacks on online services are also occurring frequently. In December there were a number of large-scale DDoS attacks of over 100 Gbps that used NTP servers as stepping stones. As seen above, the Internet continues to experience many security-related incidents.

1.2 Incident Summary

Here, we discuss the IIJ handling and response to incidents that occurred between October 1 and December 31, 2013. Figure 1 shows the distribution of incidents handled during this period*1.

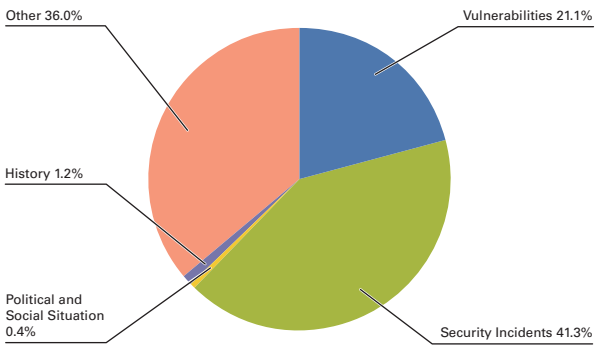


Figure 1: Incident Ratio by Category (October 1 to December 31, 2013)

The Activities of Anonymous and Other Hacktivists

Attacks by hacktivists such as Anonymous continued during this period. DDoS attacks and information leaks occurred at government-related and company sites in a large number of countries stemming from a variety of incidents and causes. In October, there were leaks of large amounts of internal data due to attacks by Anonymous (OpGoldenDawn) in countries such as Greece, Poland, and Ukraine, as well as the Organization for Security and Cooperation in Europe (OSCE). In November, there was a spate of DDoS attacks on Australian websites by Indonesia's Anonymous in protest of Australian intelligence agencies' espionage activities towards the Indonesian government. There were also

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

threats of attacks by Anonymous targeting the websites of a number of Japanese government agencies (OpKillingBay). Although it was confirmed that information, including some configuration data, leaked from a Japanese site in December, no organized attack activity was observed. Other attacks by hacktivists such as Anonymous continued on government and government-related websites around the world, centered on South America and Europe. There have also been ongoing domain hijackings, website defacements, and SNS account takeover attacks carried out by someone claiming affiliation with the Syrian Electronic Army.

■ Vulnerabilities and their Handling

During this period fixes were released for Microsoft's Windows*2*3*4*5*6, Internet Explorer*7*8*9, and Office*10. Updates were also made to Adobe Systems' Flash Player, Reader, Acrobat, and Shockwave Player. A regular quarterly update was released for Oracle's Java, fixing many vulnerabilities. A vulnerability that allowed arbitrary program execution was discovered and fixed in JustSystems Corporation's Ichitaro. Several of these vulnerabilities were exploited in the wild before patches were released*11.

Regarding server applications, a quarterly update was released for a number of Oracle products, including the Oracle database server, fixing many vulnerabilities. A vulnerability in the Windows version of the BIND9 DNS server that caused the localnets Access Control List for named to be configured incorrectly was also fixed.

A number of vulnerabilities in the popular Web application framework Ruby on Rails, including those that could allow cross-site scripting, were discovered and fixed*12. Multiple vulnerabilities were also discovered and fixed in the Apache Struts Web application framework, such as those that bypassed access control through access via certain parameters*13. A vulnerability in the Joomla! CMS that allowed the upload of arbitrary files was also fixed*14.

■ Attacks on TLD

Numerous attacks on domain registries including ccTLD continue to occur, along with associated domain hijackings and information leaks. In October, the MYNIC ccTLD registry that manages Malaysia's .my domains was accessed by an unknown entity without authorization, and a number of well-known domains including those for Microsoft and Dell were hijacked. A number of well-known domains under Costa Rica's .cr top-level domain were also hijacked. The domains of multiple prominent sites such as Google and Facebook were also hijacked after the domains.qa ccTLD registry that manages Qatar's .qa domains was accessed without authorization. A number of .rw domains for Rwanda in Africa, including notable ones such as Twitter, Google, and Facebook, were also hijacked after unauthorized access by an unidentified attacker. Additionally, in October there were a series of domain hijackings by an unknown entity that targeted a large number of corporate sites, including a hosting provider and multiple anti-virus vendors, security vendors, and SNS providers. These incidents were concentrated on a number of registrars.

*2 "Microsoft Security Bulletin MS13-081 - Critical: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2870008)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-081).

*3 "Microsoft Security Bulletin MS13-083 - Critical: Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2864058)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-083).

*4 "Microsoft Security Bulletin MS13-089 - Critical: Vulnerability in Windows Graphics Device Interface Could Allow Remote Code Execution (2876331)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-089).

*5 "Microsoft Security Bulletin MS13-090 - Critical: Cumulative Security Update of ActiveX Kill Bits (2900986)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-090).

*6 "Microsoft Security Bulletin MS13-099 - Critical: Vulnerability in Microsoft Scripting Runtime Object Library Could Allow Remote Code Execution (2909158)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-099).

*7 "Microsoft Security Bulletin MS13-080 - Critical: Cumulative Security Update for Internet Explorer (2879017)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-080).

*8 "Microsoft Security Bulletin MS13-088 - Critical: Cumulative Security Update for Internet Explorer (2888505)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-088).

*9 "Microsoft Security Bulletin MS13-097 - Critical: Cumulative Security Update for Internet Explorer (2898785)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-097).

*10 "Microsoft Security Bulletin MS13-096 - Critical: Vulnerability in Microsoft Graphics Component Could Allow Remote Code Execution (2908005)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-096).

*11 For example, IPA issued the following warning "Targeted attacks on organizations in Japan exploiting a vulnerability (CVE-2013-3906) in Microsoft Office, etc., confirmed - beware of suspicious mail, and take urgent action" (http://www.ipa.go.jp/security/topics/alert20131120.html) (in Japanese).

*12 Ruby on Rails, "Rails 3.2.16 and 4.0.2 have been released!" (http://weblog.rubyonrails.org/2013/12/3/Rails_3_2_16_and_4_0_2_have_been_released/).

*13 The Apache Software Foundation., "S2-018: Broken Access Control Vulnerability in Apache Struts2" (http://struts.apache.org/release/2.3.x/docs/s2-018.html).

*14 US-CERT, "Joomla! Media Manager allows arbitrary file upload and execution" (http://www.kb.cert.org/vuls/id/639620).

October Incidents

1 **1st:** The Ministry of Internal Affairs and Communications announced it would implement a public-private coordination project (ACTIVE) together with a number of ISPs and security vendors. This project will carry out proof-of-concept tests for preventing access to malware distribution sites as an initiative to avoid user malware infections and remove malware.
"Implementing ACTIVE and Holding ACTIVE Promotion Forum" (http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/131001_04.html).

2 **2nd:** Some federal offices were closed due to the U.S. Congress failing to establish a provisional budget, leading to a number of government-related sites, such as the site for the National Institute of Standards and Technology (NIST), going offline. These measures were lifted on October 17.

3 **3rd:** GitHub was targeted by a large-scale DDoS attack that intermittently interrupted service until the following day.
See the following GitHubStatus message from October 3 for more information. "Status Messages" (https://status.github.com/messages/2013-10-3).

4 **3rd:** The Federal Bureau of Investigation (FBI) took down the Silk Road underground site that used the Tor network, and arrested the suspect behind it.
See the following Krebs on Security Blog post for more information. "Feds Take Down Online Fraud Bazaar 'Silk Road', Arrest Alleged Mastermind" (http://krebsonsecurity.com/2013/10/feds-take-down-online-fraud-bazaar-silk-road-arrest-alleged-mastermind/).

5

6

7 **4th:** Adobe announced that its system had been compromised, and it suspected that the information of 2.9 million users and source code for a number of products had leaked.
See the following Adobe announcement for more information. "Important Customer Security Announcement" (http://blogs.adobe.com/conversations/2013/10/important-customer-security-announcement.html).

8 **8th:** The sites of a number of anti-virus vendors, including ESET in Slovakia, Bitdefender in Romania, and Avira in Germany, were targeted in domain hijackings carried out by a person or persons unknown.
See the following blog post by AVG, which was one of the affected companies, for more information. "Website issue, Tuesday 8 October" (http://blogs.avg.com/news-threats/website-issue-tuesday-8-october/).

9 **8th:** Ten international Internet-related organizations met to discuss new issues raised by the Internet, and released the "Montevideo Statement on the Future of Internet Cooperation" with regard to these issues.
"Montevideo Statement on the Future of Internet Cooperation" (http://www.icann.org/en/news/announcements/announcement -07oct13-en.htm).

10 **9th:** Microsoft published their Security Bulletin Summary for October 2013, and released four critical updates including MS13-080, MS13-081, and MS13-083, as well as four important updates.
"Microsoft Security Bulletin Summary for October 2013" (http://technet.microsoft.com/en-us/security/bulletin/ms13-oct).

11 **9th:** A number of vulnerabilities in Adobe Reader and Acrobat that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB13-25: Security updates available for Adobe Reader and Acrobat" (http://www.adobe.com/support/security/bulletins/apsb13-25.html).

12 **11th:** An unidentified attacker hijacked Google's website for Malaysia's .my domain and redirected traffic to another website.
See the following MYNIC announcement for more information about this incident. "MYNIC Official Announcement" (http://mynic.my/en/news.php?id=162).

13 **12th:** Two sites belonging to U.S. security vendor Rapid7, Metasploit.com and Rapid7.com, were targeted in a domain hijacking by an unknown entity.
See the following Kaspersky Lab Threatpost for more information. "Phony Order Faxed to Registrar Leads to Metasploit Defacement" (http://threatpost.com/phony-order-faxed-to-registrar-leads-to-metasploit-defacement/102576).

14 **13th:** It was announced that it was possible to bypass configuration screen authentication in a number of D-Link router products by setting a specific User-Agent string, and a fix was released.
CERT/CC, "Vulnerability Note VU#248083 D-Link routers authenticate administrative access using specific User-Agent string" (http://www.kb.cert.org/vuls/id/248083).

15 **15th:** A group or individual accessed Costa Rica's .cr domains without authorization, and the domains of a number of well-known sites such as Google and Yahoo! were hijacked.

16 **16th:** Oracle released their quarterly scheduled update for a number of products including Oracle, fixing a total of 127 vulnerabilities.
From this scheduled update fixes to Java vulnerabilities (51) are also included. "Oracle Critical Patch Update Advisory - October 2013" (http://www.oracle.com/technetwork/topics/security/cpuoct2013-1899837.html).

17 **19th:** The domains.qa ccTLD registry for Qatar's .qa domains was accessed without authorization by an unknown entity, and the domains of a number of well-known sites such as Google and Facebook were hijacked.

18 **25th:** Rwanda's .rw domains were accessed without authorization by an unknown party, and the domain for Google's site was hijacked.
See the following Umbrella Security Labs blog post for more information. "THE GOOGLE.RW HIJACK NOBODY ELSE NOTICED" (http://labs.umbrella.com/2013/10/25/google-rw-hijack-nobody-else-noticed/).

19 **25th:** It was reported that IDs and passwords used to connect to the Internet were being stolen from general households and used in cyber attacks. It is believed this was caused by home routers with a vulnerability that was disclosed in 2012, and widespread warnings were issued due to 300,000 of these routers having been shipped.
See the following NHK "Kabun" blog post for more information. "Over 150 Incidents of Misuse of Household Internet IDs" (http://www9.nhk.or.jp/kabun-blog/1000/171059.html) (in Japanese). Telecom-ISAC Japan had also issued a warning regarding this vulnerability in July 2012. "[Warning] Logitec Brand Router Vulnerability, and Steps to be Taken by Users" (https://www.telecom-isac.jp/news/news20120730.html) (in Japanese).

20

21

22

23

24

25

26

27

28

29

30

31 **31st:** JPCERT/CC established a site that enabled users to check whether or not network devices such as DNS servers or broadband routers in their environment were open resolvers.
JPCERT Coordination Center, "Announcement of Site for Checking Open Resolvers" (http://www.jpcert.or.jp/pr/2013/pr130002.html) (in Japanese).

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

*Dates are in Japan Standard Time

■ Attacks Targeting IDs and Passwords, and Unauthorized Login through Identity Fraud

During this survey period there were ongoing attempts to steal user IDs and passwords, and login without authorization through identity fraud presumably using lists of these IDs and passwords. Similar activity has been observed frequently since about March 2013. There were a large number of unauthorized login attempts on member-oriented service sites such as mobile SNS, as well as websites including point services, e-commerce sites, and card member service sites, thought to have used lists of ID and password combinations.

There was also an incident of unauthorized access at Adobe in October, leading to information on their customers as well as the source code for some of their products leaking. This was a major leak initially thought to involve the personal information of 2.9 million customers, but a subsequent investigation revealed that information on at least 38 million customers was affected. Additionally, because this member information was published to the Internet by an unknown entity, Facebook and a number of other companies temporarily suspended the accounts of users who were on the list, and prompted them to change their password*15. These ongoing incidents of unauthorized access thought to use lists of IDs and passwords demonstrate that continued vigilance is necessary.

■ Government Agency Initiatives

Initiatives and new services using big data have attracted a lot of attention lately. However, at the same time a variety of issues regarding the use, application and privacy of big data that includes personal data, such as the purchase history of consumers and usage history of digital currency, have been identified and discussed. In a "Statement on Forging a World-Leading IT Nation*16" approved by cabinet in June 2013, the government declared it would promote the more proactive use and application of IT and data. From September 2013, the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (IT Strategic Headquarters) held discussions at the Investigative Commission on Personal Data*17 as well as its Technical Evaluation Working Group to investigate and evaluate the clarification of rules on the use and application of personal data.

In December, a "Proposal for the Review of Systems Regarding the Use and Application of Personal Data" was drawn up. This clarified the scope of protected personal data, classified data processed to reduce the likelihood of the individual being identified as not requiring said person's permission when providing it to third parties, and introduced legal measures regarding the obligations of companies that handle this data. The proposal also advocated an overhaul of systems for protecting personal data, including the establishment of an independent, third-party organization. To that end, the proposal was adopted at the 63rd meeting of the IT Strategic Headquarters, which was held on December 20. In the months ahead legislation will be developed, including amendments to the Personal Information Protection Law, while examining and defining issues.

From November, the Ministry of Internal Affairs and Communications held a "Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business." This concerns responses by telecommunications carriers based on guidelines*18. The goal of the workshop is to evaluate how to appropriately deal with increasingly sophisticated and complex cyber attacks when necessary, to enable telecommunications carriers to implement new measures and initiatives while respecting the confidentiality of communications.

■ Concerning the NSA

Western media companies have reported on mass surveillance by the National Security Agency (NSA) and its affiliates since June, and during this survey period a wealth of new information came to light. In particular, reports on wiretapping in European countries, the wiretapping of leaders of countries around the world, and wiretapping by U.S. embassies led to criticism of these U.S. and U.K. activities in the countries involved, and there are concerns that it could affect foreign diplomacy.

*15 See the following Krebs on Security blog post for more information, "Facebook Warns Users After Adobe Breach" (http://krebsonsecurity.com/2013/11/facebook-warns-users-after-adobe-breach/).
*16 "Regarding the Statement on Forging a World-Leading IT Nation" (http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20130614/siryou1.pdf) (in Japanese).
*17 "Investigative Commission on Personal Data" (http://www.kantei.go.jp/jp/singi/it2/pd/index.html) (in Japanese).
*18 Four telecommunications business-related organizations, "Guidelines for Dealing with High Volume Communications and Privacy at Telecommunications Carriers - Second Edition" (http://www.jaipa.or.jp/other/mtcs/110325_guideline.pdf) (in Japanese).

November Incidents

6th: Microsoft published an advisory due to a vulnerability in the Microsoft Graphics component (CVE-2013-3906) that could allow remote code execution via specially-crafted files. It was confirmed that attacks exploiting this vulnerability had already been made by the time it was disclosed.
"Microsoft Security Advisory (2896666) Vulnerability in Microsoft Graphics Component Could Allow Remote Code Execution" (http://technet.microsoft.com/en-us/security/advisory/2896666).

6th: Apple published its first Transparency Report, which covered the period from January to June 2013.
"Report on Government Information Requests" (http://images.apple.com/pr/pdf/131105reportongovinforequests3.pdf).

8th: IPA published a warning about the issue of information on office devices such as all-in-one printers being viewable from the Internet, recommending measures such as not connecting them to networks unless required, and managing them appropriately.
"Press Release - Important Points When Connecting Office Devices Such as All-in-One Printers to the Internet" (http://www.ipa.go.jp/about/press/20131108.html) (in Japanese).

12th: A vulnerability in JustSystems Corporation's Ichitaro software product that could allow arbitrary code execution via specially-crafted files was discovered and fixed. It was confirmed that attacks exploiting this vulnerability had been made before a patch was released.
"[JS13003] Regarding the Risk of Malicious Program Execution Exploiting a Vulnerability in Ichitaro" (http://www.justsystems.com/jp/info/js13003.html) (in Japanese).

13th: Microsoft released the Enhanced Mitigation Experience Toolkit (EMET) 4.1, which is a security tool for mitigating application vulnerabilities.
See the following TechNet Blogs post for more information. "Introducing Enhanced Mitigation Experience Toolkit (EMET) 4.1" (http://blogs.technet.com/b/srd/archive/2013/11/12/introducing-enhanced-mitigation-experience-toolkit-emet-4-1.aspx).

13th: A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB13-26 Security updates available for Adobe Flash Player" (http://www.adobe.com/support/security/bulletins/apsb13-26.html).

13th: Microsoft published their Security Bulletin Summary for November 2013, and released three critical updates, MS13-088, MS13-089, and MS13-090, as well as five important updates.
"Microsoft Security Bulletin Summary for November 2013" (http://technet.microsoft.com/en-us/security/bulletin/ms13-nov).

13th: Anonymous announced OpKillingBay, threatening attacks on Japanese government agencies and related organizations.

14th: A number of research institutions, including Kyoto University, University of Tsukuba, and the High Energy Accelerator Research Organization, announced that each of their supercomputer systems had been accessed from outside without authorization.
See the following High Energy Accelerator Research Organization (KEK) announcements for more information.
"On unauthorized access to a computing system at KEK" (http://legacy.kek.jp/intra-e/info/2013/111515/).
"On unauthorized access to a computer system at KEK (Follow-up)" (http://legacy.kek.jp/intra-e/info/2013/121017/).

18th: A technical expert in the U.K. announced that LG's Smart TVs (televisions with network functionality) were sending usage information without the users' intent.
See the following blog post by the discoverer for more information. DoctorBeet's Blog, "LG Smart TVs logging USB filenames and viewing info to LG servers" (http://doctorbeet.blogspot.ru/2013/11/lg-smart-tvs-logging-usb-filenames-and.html).

19th: There was an incident of unauthorized login to GitHub via brute force attacks.
See the following GitHub blog post for more details. "Weak passwords brute forced" (https://github.com/blog/1698-weak-passwords-brute-forced).

20th: IPA issued a warning regarding a vulnerability in the Microsoft Graphics component (CVE-2013-3906) that Microsoft disclosed on November 6. It was confirmed that attack emails with attachments such as "履歴書.zip" (meaning "resume") that exploited this vulnerability had been sent to organizations in Japan.
"Targeted attacks on organizations in Japan exploiting a vulnerability (CVE-2013-3906) in Microsoft Office, etc., confirmed - beware of suspicious mail, and take urgent action" (http://www.ipa.go.jp/security/topics/alert20131120.html) (in Japanese).

23rd: Twitter announced it had enabled forward secrecy for SSL communications to enhance the protection of user information.
Twitter, Inc, Engineering Blog, "Forward Secrecy at Twitter" (https://blog.twitter.com/2013/forward-secrecy-at-twitter-0).

28th: Microsoft published an advisory regarding a vulnerability in the kernel component of Windows XP and Windows Server 2003 (CVE-2013-5065) that could allow remote code execution.
"Microsoft Security Advisory (2914486) Vulnerability in Microsoft Windows Kernel Could Allow Elevation of Privilege" (http://technet.microsoft.com/en-us/security/advisory/2914486).

29th: The Ministry of Internal Affairs and Communications held a Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business to evaluate how to appropriately deal with cyber attacks in the field of telecommunications.
"Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business" (http://www.soumu.go.jp/main_sosiki/kenkyu/denki_cyber/index.html) (in Japanese)

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

*Dates are in Japan Standard Time

In response to this, ten Internet-related organizations jointly issued the "Montevideo Statement on the Future of Internet Cooperation" in October, indicating their deep concern at the fact that users all over the world have lost their faith and confidence in the Internet. In December, the United Nations also unanimously voted to adopt a resolution entitled "The right to privacy in the digital age," calling on countries to protect the privacy of individuals, including with regard to digital communications. Additionally, Yahoo! and Google were put under pressure when it was reported that the NSA was intercepting communications between their data centers. Service providers rushed to implement measures to counter the interception of communications, such as encrypting communications that were previously conducted using plain text, and enabling support for Perfect Forward Secrecy (PFS). See "1.4.2 Forward Secrecy" for more information about PFS.

In December, seven major IT companies affected by this situation began calling for legal restrictions on government surveillance and the abolishment of regulations limiting communication. Additionally, a U.S. presidential advisory committee, which was investigating data gathering activities by intelligence agencies as a result of these issues, recommended that reforms be carried out while retaining functionality necessary for security, as they considered that intelligence gathering activities had gone too far.

■ Cloud Service Usage and Risks

In recent years, functions and services that use cloud environments, such as online storage and online groupware, have been on the rise. The use of these functions is becoming more widespread, due to the convenience of them being available from a variety of locations and devices when needed. Meanwhile, in some cases use of these functions in the workplace may require caution. For example, in July 2013 there were incidents of information not meant for the public eye as well as confidential information leaking at a number of government ministries, due to the use of group email services provided by private sector companies that had mistakenly been configured as publicly accessible*19.

During this survey period, cloud functions for the Japanese IME (Input Method Editor) became a topic of discussion. The IME is a function required in environments that handle multibyte characters. Recently, more and more of these IMEs have cloud-related functions implemented that require an always-on Internet connection. These cloud functions provide functionality such as displaying conversion candidates or sharing user dictionaries over multiple devices based on user input. For some Japanese IMEs, it was found that certain details input by users were transmitted regardless of settings. In these incidents data was transmitted due to bugs, but a number of the affected IME tools were pre-installed on computers or mobile devices, or bundled with other software in some cases, and depending on the circumstances it was possible that they were being used without the user's intention. As a result, fixes were made to patch the bugs and disable the use of cloud functions under default settings.

These functions are extremely useful, but as the data input or registered was transmitted externally, they could situationally lead to information leaks occurring. That means they must be used with caution, especially at organizations such as companies*20.

■ Bitcoin

As transactions using the Bitcoin*21 virtual currency become more widespread, a variety of incidents are occurring. During the current survey period, the Silk Road underground site that carried out transactions using Bitcoin was taken down by the FBI, and the site's owner was arrested on suspicion of violation of anti-drug laws. Silk Road is thought to have facilitated the trade of illegal drugs and other illegal transactions. When it was shut down, approximately 30,000 XBT (Bitcoin trading units) were seized. There has also been a rash of attacks on virtual currency exchanges and account management services, involving many DDoS attacks, as well as server compromises in which bitcoins and site account information were stolen.

*19 More information can be found at the Council for Promotion of Information Security Measures (Liaison Conference for CISO, etc.) held at the National Information Security Center. "11th Assembly (July 11, 2013)" (http://www.nisc.go.jp/conference/suishin/index.html#2013_3) (in Japanese).

*20 IIJ has also issued a warning regarding cloud-related IME functions in the IIJ-SECT Security Diary. "Warnings on the Use of the Online Functions of an IME" (https://sect.iij.ad.jp/en/d/2013/12/104971.html).

*21 See Vol.21 (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol21_EN.pdf) of this report under "1.4.3 The Bitcoin Virtual Currency" for more information about Bitcoin.

December Incidents

1 V **4th:** A number of vulnerabilities in Ruby on Rails, including cross-site scripting, were discovered and fixed.
"Rails 3.2.16 and 4.0.2 have been released!" (http://weblog.rubyonrails.org/2013/12/3/Rails_3_2_16_and_4_0_2_have_been_released/).

2 S **6th:** Microsoft's Digital Crime Unit (DCU) announced it had initiated a takedown of the ZeroAccess botnet in collaboration with a number of investigative organizations such as the FBI and Europol as well as companies.
See the following Microsoft announcement for more details. "Microsoft, the FBI, Europol and industry partners disrupt the notorious ZeroAccess botnet" (http://www.microsoft.com/en-us/news/press/2013/dec13/12-05zeroaccessbotnetpr.aspx).

3 4 5 O **6th:** Microsoft announced measures such as stronger encryption for their products and services in response to the government's monitoring of the Internet.
See the following Microsoft blog post for more information "Protecting customer data from government snooping" (http://blogs.technet.com/b/microsoft_blog/archive/2013/12/04/protecting-customer-data-from-government-snooping.aspx").

6 S **8th:** It was revealed that a number of Google domain certificates had been fraudulently issued at an intermediate authority affiliated with France's government certificate authority ANSSI. As a result, the corresponding certificates were revoked in a number of browsers. It is claimed that this was caused by human error.
See the following ANSSI announcement for more details. "Revocation of an IGC/A branch" (http://www.ssi.gouv.fr/en/the-anssi/events/revocation-of-an-igc-a-branch-808.html).

7 8 O **9th:** The National Information Security Center held the "CIIREX 2013" interdisciplinary exercise for critical infrastructure.
"Summary of Interdisciplinary Exercise for Critical Infrastructure [CIIREX 2013]" (http://www.nisc.go.jp/active/infra/pdf/ciirex2013_2.pdf) (in Japanese).

9 10 O **10th:** Seven major U.S. IT companies including Google and Microsoft jointly began initiatives calling for legal restriction on government surveillance and the abolishment of regulations limiting communications.
Their action policy and petitions to the U.S. President and the federal government have been published on the following site. Reform Government Surveillance (http://reformgovernmentsurveillance.com/).

11 V **11th:** Microsoft published their Security Bulletin Summary for December 2013, and released five critical updates including MS13-096, MS13-097, and MS13-099, as well as six important updates.
"Microsoft Security Bulletin Summary for December 2013" (http://technet.microsoft.com/en-us/security/bulletin/ms13-dec).

12 13 V **11th:** A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB13-28: Security updates available for Adobe Flash Player" (http://helpx.adobe.com/security/products/flash-player/apsb13-28.html).

14 15 V **12th:** Vulnerabilities in PHP, including those that could allow code execution or system termination due to memory corruption occurring when a fraudulent certificate is processed in the OpenSSL module (CVE-2013-6420), were discovered and fixed.
NVD, "Vulnerability Summary for CVE-2013-6420" (https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-6420).

16 17 O **12th:** The 14th assembly of the Council for Promotion of Information Security Measures (Liaison Conference for CISO, etc.) was held, and survey results on the use and measures in place for Windows XP and all-in-one printers at each government were presented.
National Information Security Center, Council for Promotion of Information Security Measures (Liaison Conference for CISO, etc.) "14th Assembly (Dec. 12, 2013)" (http://www.nisc.go.jp/conference/suishin/index.html#2013_6) (in Japanese).

18 V **17th:** A vulnerability in Google's Android OS that could allow execution of Android OS functions or arbitrary code from arbitrary Java methods was discovered and fixed.
JVN. "JVN#53768697 Android OS vulnerable to arbitrary Java method execution"(https://jvn.jp/en/jp/JVN53768697/index.html).

19 O **17th:** The statute of limitation expired for incidents of malware infection via targeted attacks on defense-related companies that came to light in September 2011. Although an investigation into charges of fraudulent obstruction of business had been carried out, no suspects were identified.

20 21 O **19th:** A U.S. presidential advisory committee published a report on the intelligence-gathering activities of the National Security Agency (NSA), and advised that limits be placed on these activities.
White House, "Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies" (http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf).

22 23 O **20th:** The United Nations unanimously voted to adopt a resolution entitled "The right to privacy in the digital age," calling on countries to protect the privacy of individuals, including with regard to digital communications.
United Nations, "General Assembly backs right to privacy in digital age" (http://www.un.org/apps/news/story.asp?NewsID=46780&Cr= privacy&Cr1=).

24 25 O **20th:** At the 63rd meeting of the Strategic Headquarters for the Promotion of Advanced Information and Telecommunications Network Society (IT Strategic Headquarters), a policy was set for revising systems for protecting personal privacy, directed at the use and application of personal data including individual information.
Cabinet, "Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (63rd Meeting) - Agenda" (http://www.kantei.go.jp/jp/singi/it2/dai63/gijisidai.html) (in Japanese).

26 P **26th:** The Prime Minister of Japan visited the Yasukuni Shrine.

27 O **26th:** It was reported that online functions of Japanese IME were sending information without users' intent in some cases.

28 29 S **27th:** It was reported that large-scale NTP reflection attacks had been observed over the Christmas season.
See the following Symantec blog post for more details. "Hackers Spend Christmas Break Launching Large Scale NTP-Reflection Attacks" (http://www.symantec.com/connect/blogs/hackers-spend-christmas-break-launching-large-scale-ntp-reflection-attacks).

30 31 S **31st:** The game servers of a number of games, such as the online game League of Legends, were targeted in DDoS attacks by a person or persons unknown.
See the following post on the Reddit social bookmarking site for more information about the attacks on League of Legends. "Servers down? Discuss here." (http://www.reddit.com/r/leagueoflegends/comments/1u1pcz/servers_down_discuss_here/).

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

*Dates are in Japan Standard Time

Bitcoin mining functions have also been found in freeware, and malware that carries out mining is spreading*22. Transactions using Bitcoin are becoming more common, to the point where their impact can no longer be ignored. The People's Bank of China issued an alert regarding Bitcoin transactions*23. As a result, BTC China temporarily suspended currency-based transactions*24. Similar warnings were also given by financial authorities in India*25, and a number of Indian exchanges stopped trading.

■ Other

Regarding malware infection incidents caused by targeted attacks on defense-related companies that were exposed in September 2011, an investigation had been carried out on suspicion of the fraudulent obstruction of business, but in December 2013 the statute of limitations expired without a suspect being identified. Targeted attacks aim to avoid discovery by covering their tracks through the deletion of activity records, etc. This means it is not only hard to tell when you are being attacked, it is also often difficult to assess damages and identify the attacker when investigating after an attack comes to light. This raises the importance of implementing internal measures such as the control of communications at the external boundary, and the design and operation of information systems. It also means that measures such as saving records appropriately are crucial*26.

There were reports that part of a cryptographic algorithm (Dual_EC_DRBG) established by the National Institute of Standards and Technology (NIST) contained a U.S. National Security Agency (NSA) backdoor, making decryption possible. In response, NIST issued a warning recommending that the corresponding encryption not be used*27. In December, it was reported that U.S. company EMC had been compensated for preferentially selecting this cryptographic algorithm for their RSA products. However, EMC denies this*28.

Also in December, Symantec reported on large-scale NTP-based DDoS attacks in its blog. This attack exploits NTP's monlist function, and in January 2014 a warning about the vulnerability was issued due to the possibility of it being used in DDoS attacks*29. Also between the end of December 2013 and the time of writing, an unknown entity made a number of DDoS attacks on game-related sites, etc., that are thought to have exploited this function, with attacks of over 100 Gbps reported. As a result, moves have been made to counter this, including the start of OpenNTPProject.org*30, which lets you check whether an NTP server that returns a response exists on a given network.

*22 See the following TrendLabs Security Blog post for more details. "The threat of a 'malicious program that mines Bitcoins' also confirmed to have infected 3,000 computers in Japan" (http://blog.trendmicro.co.jp/archives/8271) (in Japanese).

*23 The People's Bank of China, "比特币相关事宜答记者问" (http://www.pbc.gov.cn/publish/goutongjiaoliu/524/2013/20131205153950799182785/20131205153950799182785_.html) (in Chinese).

*24 BTC China "An Open Letter from Bobby Lee, CEO of BTC China" (https://vip.btcchina.com/page/notice20131220).

*25 The Reserve Bank of India, "RBI cautions users of Virtual Currencies against Risks" (http://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=30247).

*26 For more information about targeted attack countermeasures, also see the Information-technology Promotion Agency, Japan's (IPA) "The System Design Guide for Thwarting Targeted Email Attacks" (http://www.ipa.go.jp/security/english/newattack_en.html).

*27 In September 2013, NIST published an advisory recommending against the use of SP 800-90A (Dual_EC_DRBG), and announcing they would make revisions. "SUPPLEMENTAL ITL BULLETIN FOR SEPTEMBER 2013 NIST OPENS DRAFT SPECIAL PUBLICATION 800-90A, RECOMMENDATION FOR RANDOM NUMBER GENERATION USING DETERMINISTIC RANDOM BIT GENERATORS, FOR REVIEW AND COMMENT" (http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf).

*28 See the following official blog post for U.S. EMC's official announcement, "RSA RESPONSE TO MEDIA CLAIMS REGARDING NSA RELATIONSHIP" (http://blogs.rsa.com/news-media-2/rsa-response/).

*29 JVN, "JVNVU#96176042 Issues with NTP being used as a stepping stone in DDoS attacks" (http://jvn.jp/vu/JVNVU96176042/) (in Japanese).

*30 OpenNTPProject.org - NTP Scanning Project (http://openntpproject.org/).

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 Protection Service between October 1 and December 31, 2013.

This information shows traffic anomalies judged to be attacks based on IIJ DDoS Protection 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*31, attacks on servers*32, and compound attacks (several types of attacks on a single target conducted at the same time).

During the three months under study, IIJ dealt with 498 DDoS attacks. This averages to 5.4 attacks per day, indicating a decrease in the average daily number of attacks compared to our prior report. Server attacks accounted for 41.6% of all incidents, while compound attacks accounted for 51.8%, and bandwidth capacity attacks 6.6%.

The largest attack observed during the period under study was classified as a compound attack, and resulted in 2.94 Gbps of bandwidth using up to 1,055,000 pps packets.

Of all attacks, 89.2% ended within 30 minutes of commencement, 10.6% lasted between 30 minutes and 24 hours, and 0.2% lasted over 24 hours. The longest sustained attack for this period was a compound attack that lasted for three days, eight hours, and 51 minutes (80 hours and 51 minutes).

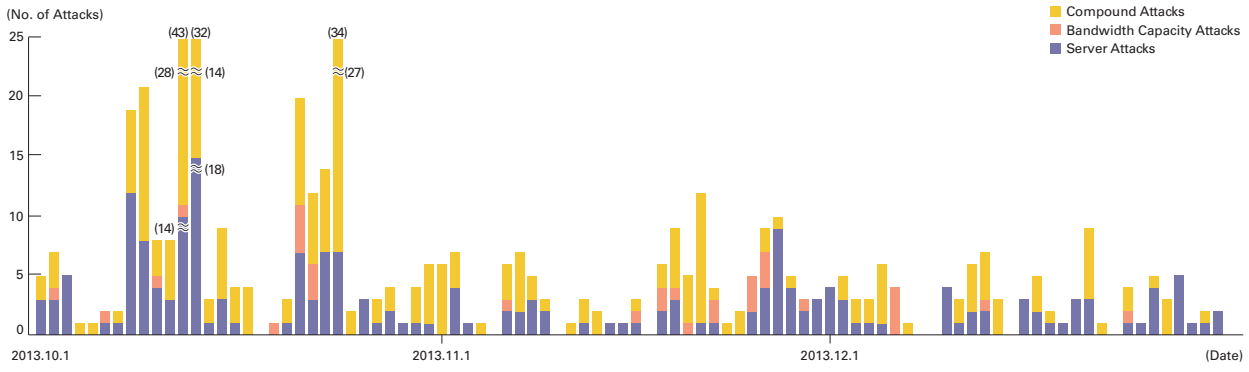


Figure 2: Trends in DDoS Attacks

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

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

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

Backscatter Observations

Next we present our observations of DDoS attack backscatter using the honeypots*35 set up by the MITF, a malware activity observation project operated by IIJ*36. By monitoring backscatter it is possible to detect some of the DDoS attacks occurring on external networks as a third party without any interposition.

For the backscatter observed between October 1 and December 31, 2013, Figure 3 shows the sender's IP addresses classified by country, and Figure 10 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 45.8% of the total during the target period. Attacks were also observed on 1935/TCP used for streaming communications, 22/TCP used for SSH, as well as 8000/TCP and 8877/TCP, which are normally not used.

Looking at the origin of backscatter thought to indicate IP addresses targeted by DDoS by country in Figure 3, for the current survey period the United States accounted for the largest ratio at 14.9%. Russia and Chile followed at 10.1% and 9.5%, respectively. During this survey period many attacks from Chile were observed, with a total of over 85,000 attacks targeting 445/TCP on a specific honeypot from a number of IP addresses.

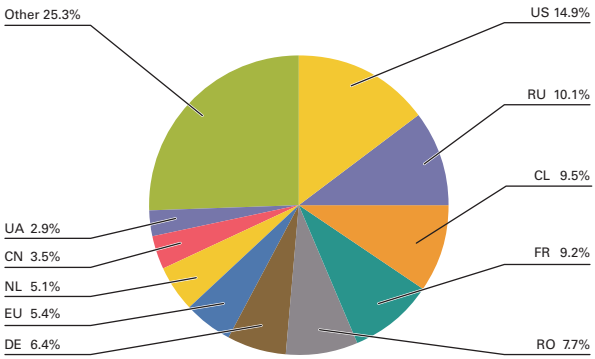


Figure 3: DDoS Attack Targets by Country According to Backscatter Observations

Regarding particularly large numbers of backscatter packets observed by targeted port, there were attacks on the Web servers (80/TCP) for a news provider in Azerbaijan on October 17. Similar attacks on this provider were also observed on October 23. On October 26, attacks on the servers of an ISP in Ukraine and a hosting provider in Romania were observed.

Many attacks from Chile were observed during this survey period, due to attacks targeting 445/TCP on a specific honeypot. A large number of attacks were observed from a number of IP addresses on December 11, 14, and 24. A total of more than 85,000 pieces of communication were

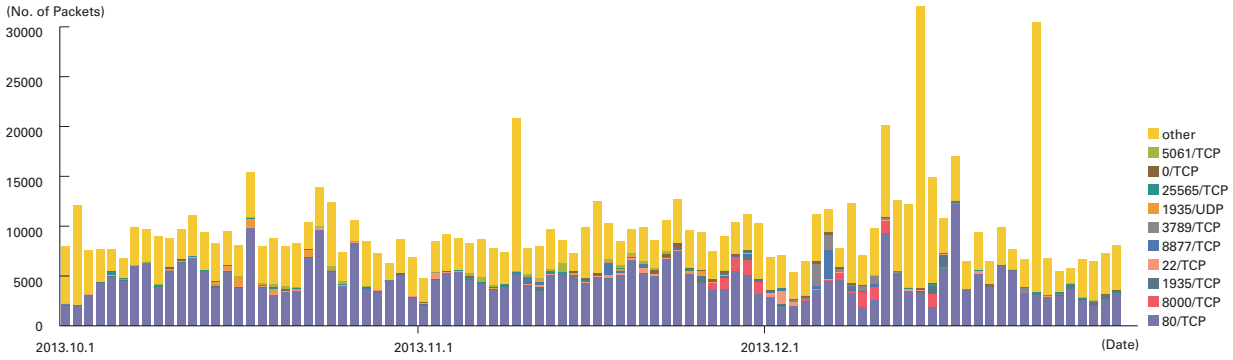


Figure 4: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)

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

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

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

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

observed. On October 2, communications thought to be port scanning targeting servers in Iran were observed. On November 9, attacks were observed on servers in Argentina. Attacks targeting 8000/TCP on the servers of a hosting provider in Germany were observed at a number of times such as November 9 and December 9. Attacks were also observed targeting 8877/TCP on the servers of a hosting provider in Russia on November 17 and December 6. These ports are not normally used by standard applications, so the purpose of the attacks is not known.

Notable DDoS attacks during the current survey period that were detected via IIJ's observations of backscatter included multiple attacks on GitHub from October, and attacks on the Web servers of Interpol Indonesia thought to have been carried out by Anonymous also in October. We also observed attacks on Russian government agencies believed to be carried out by Anonymous in November, and attacks on financial institutions in the U.K. in December.

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the MITF*37, a malware activity observation project operated by IIJ. The MITF uses honeypots*38 connected to the Internet in a manner similar to general users in order to observe communications arriving over the Internet. Most appear to be communications by malware selecting a target at random, or scans attempting to locate a target for attack.

Status of Random Communications

Figure 5 shows the distribution of sender's IP addresses by country for communications coming into the honeypots between October 1 and December 31, 2013. 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.

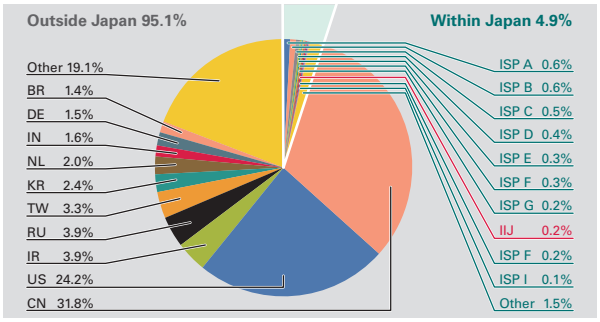


Figure 5: Sender Distribution (by Country, Entire Period under Study)

Much of the communications arriving at the honeypots demonstrated scanning behavior targeting TCP ports utilized by Microsoft operating systems. We also observed scanning behavior targeting 1433/TCP used by Microsoft's SQL Server, 3389/TCP used by the RDP remote login function for Windows, 22/TCP used for SSH, 80/TCP used for HTTP, ICMP echo requests, and 53/UDP used for DNS.

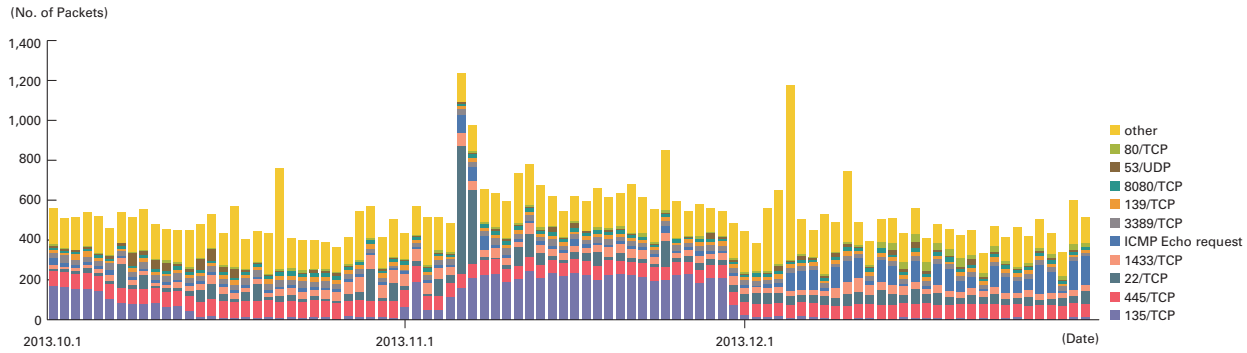


Figure 6: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

*37 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.

*38 A system designed to simulate damages from attacks by emulating vulnerabilities, recording the behavior of attackers, and the activities of malware. Communications thought to be SSH dictionary attacks also occurred during the current survey period.

Communications thought to be SSH dictionary attacks also occurred during the current survey period. For example, communications that occurred between November 6 and November 7 came from IP addresses allocated to China. Communications since mid-September thought to be scanning for open DNS resolvers have continued, also occurring in October and December*39. During the current survey period, we have also observed similar scanning communications in large volumes from IP addresses allocated to the Netherlands and the United States in addition to China. About twice the normal volume of communications has been targeting 1433/TCP, with most originating from IP addresses allocated to China. In each case, communications targeted an extremely wide range of IP addresses, suggesting that these are continued attempts to find targets to attack or exploit as stepping stones in attacks. Communications targeting 135/TCP from IP addresses allocated to the United States that demonstrated scanning behavior for RPC servers are also ongoing, and were observed on a large scale in early to mid-October, as well as in November.

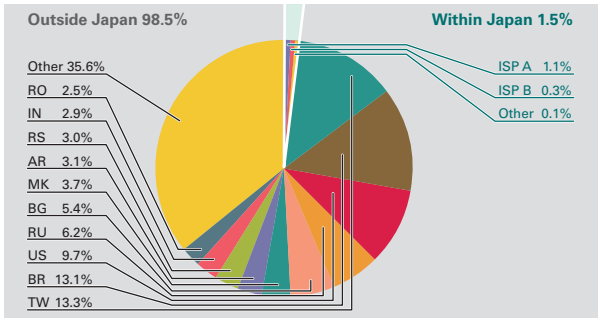


Figure 7: Distribution of Acquired Specimens by Source (by Country, Entire Period under Study, Excluding Conficker)

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

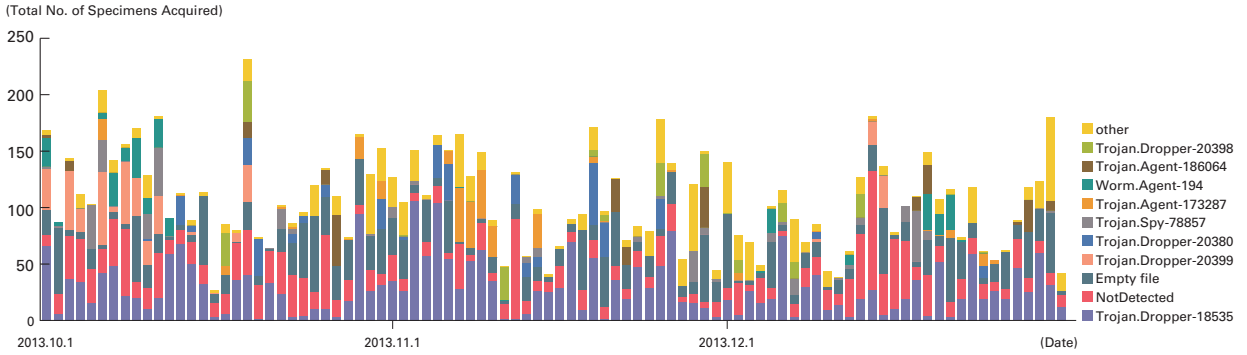


Figure 8: Trends in the Total Number of Malware Specimens Acquired (Excluding Conficker)

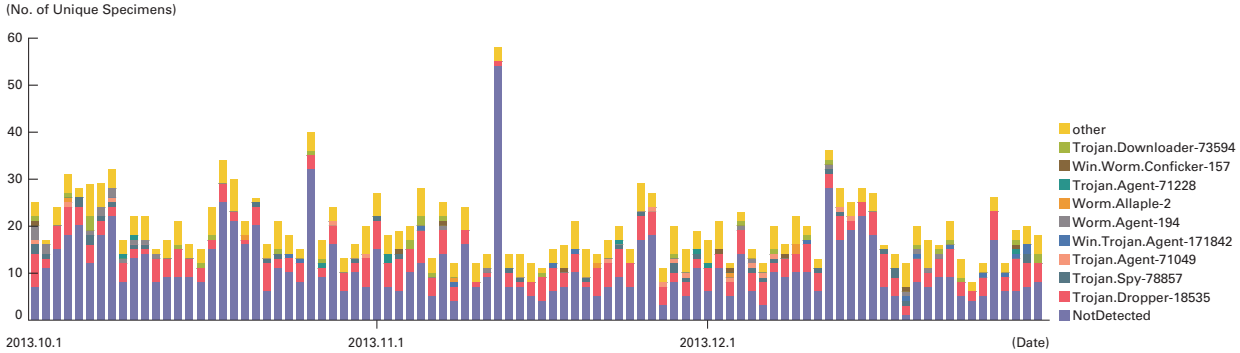


Figure 9: Trends in the Number of Unique Specimens (Excluding Conficker)

*39 For example, we confirmed that communications observed on October 8 were scans from the same source reported in CNotes "DNS amp - source address 2" (http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=DNS+amp+-+source+address+2) (in Japanese).

acquired per day*40, while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*41.

Specimens are also identified using anti-virus software, and a breakdown of the top 10 variants is displayed color coded by malware name. As with our previous report, for Figure 8 and Figure 9 we have detected Conficker using multiple anti-virus software packages, and removed any Conficker results when totaling data.

On average, 108 specimens were acquired per day during the period under study, representing 20 different malware. After investigating undetected specimens more closely, worms*42 from IP addresses allocated to a number of countries such as the United States were observed on an ongoing basis, along with a type of bot*43 controlled via IRC server from IP addresses allocated to the Philippines. Approximately two-thirds of the undetected specimens during this survey period were text format (about 30% in the last survey period). Because many of these text format specimens were HTML 404 or 403 error responses from Web servers, we believe this was due to infection behavior of malware such as old worms continuing despite the closure of download sites that newly-infected PCs access to download malware.

Under the MITF's independent analysis, during the current period under observation 89.2% of malware specimens acquired were worms, 4.4% were bots, and 6.4% were downloaders. In addition, the MITF confirmed the presence of 16 botnet C&C servers*44 and 6 malware distribution sites.

■ Conficker Activity

Including Conficker, an average of 36,340 specimens were acquired per day during the period covered by this report, representing 756 different malware. While figures rise and fall over short periods, Conficker accounts for 99.7% of the total number of specimens acquired, and 97.3% of unique specimens. This demonstrates that Conficker remains the most prevalent malware by far, so we have omitted it from figures in this report.

The total number of specimens acquired during the period covered by this report increased by approximately 6% compared to the previous survey period. Unique specimens were down by about 4%. According to the observations of the Conficker Working Group*45, as of December 31, 2013, a total of 1,267,162 unique IP addresses are infected. This is a drop of approximately 40% compared to the 3.2 million PCs observed in November 2011, but it demonstrates that infections are still widespread.

*40 This indicates the malware acquired by honeypots.

*41 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.

*42 WORM_ATAK (http://about-threats.trendmicro.com/archiveMalware.aspx?language=jp&name=WORM_ATAK.D).

*43 BKDR_QAKBOT (http://about-threats.trendmicro.com/malware.aspx?language=en&name=BKDR_QAKBOT).

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

*45 Conficker Working Group Observations (http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking).

1.3.3 SQL Injection Attacks

Of the types of different Web server attacks, IIJ conducts ongoing surveys related to SQL injection attacks*46. SQL injection attacks have flared up in frequency numerous times in the past, remaining one of the major topics in the Internet security. SQL injections are known to occur in one of three attack patterns: those that attempt to steal data, those that attempt to overload database servers, and those that attempt to rewrite Web content.

Figure 10 shows the distribution of SQL injection attacks against Web servers detected between October 1 and December 31, 2013. Figure 11 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 46.4% of attacks observed, while the United States and China accounted for 20.8% and 9.9%, 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 this period, large-scale attacks from multiple attack sources in South Korea directed at specific targets took place on November 7. On October 1, attacks were made on specific targets from attack sources in a number of countries/regions, including Hong Kong and the United States. On October 9, attacks were made on specific targets from sources in multiple countries, including the United States and Germany. On November 21, there were attacks from specific attack sources in Japan on specific targets, as well as attacks from specific attack sources in the United States on specific targets. On December 21, there were attacks from a number of attack sources in Japan directed at specific targets. These attacks are thought to have been attempts to find vulnerabilities on Web servers.

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

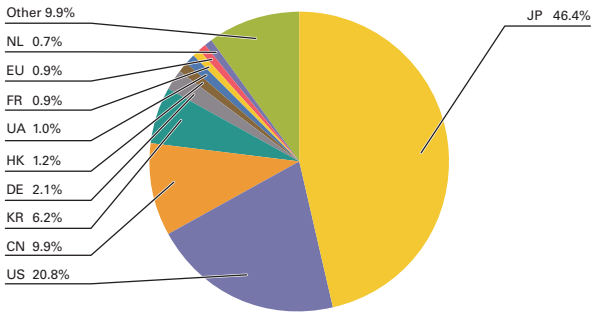


Figure 10: Distribution of SQL Injection Attacks by Source

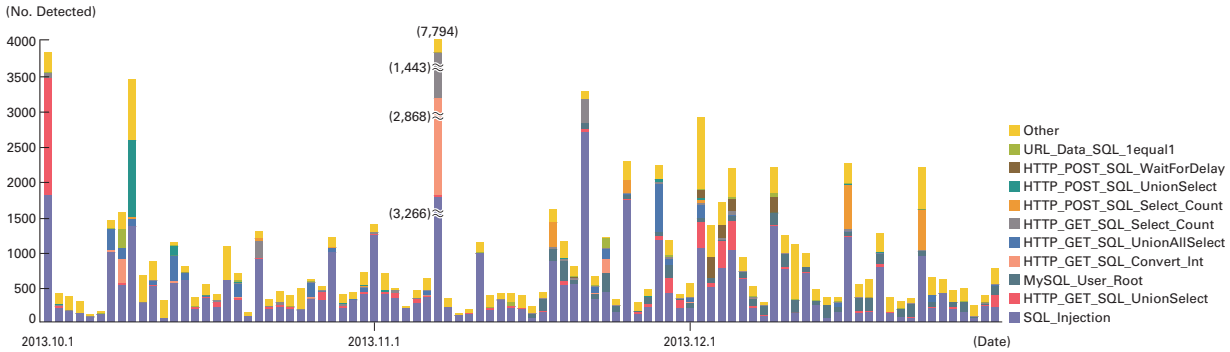


Figure 11: Trends in SQL Injection Attacks (by Day, by Attack Type)

*46 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 covering three themes, including points to note regarding memory forensics for devices equipped with large amounts of memory, as well as discussion of forward secrecy, and website defacement surveys carried out using Web crawlers.

1.4.1 Points to Note Regarding Memory Forensics for Devices with Large Amounts of Memory

As PCs become more and more powerful, hard disk and memory capacities are also continuing to grow. Efficiently analyzing media that now has such large capacities is one of the challenges of digital forensics. It is not very well known, but as capacities grow larger, forensic analysis of volatile memory data can be rendered impossible. In this section we examine the reasons for this, and discuss points to note regarding the memory forensics tools used. Note that the memory forensics discussed here only applies to Windows OSes.

■ The Cause of This Phenomenon

Before explaining the phenomenon at issue, we will give a basic explanation of memory forensics*47. Like disk forensics, memory forensics consists of two phases: the initial "acquisition" process to save the binary data in the memory in its entirety, followed by "analysis," in which information is extracted independently from the data acquired. The binary data acquired from the memory is called a memory image. There are three types of memory image: raw (memory data extracted as-is), crash dump (memory data with the space reserved by hardware removed, and a header added at the start), and hibernation (compressed memory data for returning from hibernation). Currently, acquisition tools only save in raw or crash dump format. Additionally, most analysis tools can only analyze raw format images, and very few can analyze crash dump or hibernation format images. Consequently, other than cases in which a hibernation format image left on a device's hard disk is analyzed, memory forensics can be thought of as a technique for acquiring and analyzing raw (or when appropriate crash dump) format memory images.

The analysis process for memory forensics involves a number of key pieces of data, but the following two in particular are required no matter what kind of information is extracted.

1. The physical offset of the conversion table for a kernel and every process, for converting virtual addresses to physical ones*48.
2. The debug structure, including pointers to the OS version and process list*49.

Analysis tools use different processes to extract these pieces of data depending on the memory image format. For raw images, they are extracted by searching the entire memory image using the signature for each piece of data. Meanwhile, for crash dump images the header at the start includes this information, so there is no need to search the data. The phenomenon at issue occurs when searching for the second item above, the debug structure, in raw format memory images. For devices that have x64 architecture Windows installed and are equipped with large amounts of memory*50, the debug structure in memory images acquired is sometimes encoded using a fixed algorithm. Consequently, analysis tools cannot find the debug structure, and analysis is aborted.

Table 1: Memory Image Acquisition Tool Test Results

	FTK Imager	Belkasoft Live RAM Capturer	Windows Memory Reader	winpmem	DumpIt
raw	Does not decode	Does not decode	Does not decode	Does not decode	Does not decode
crashdump	-	-	Does not decode	Does not decode	Decodes

*47 IIJ-SECT Security Diary has discussed techniques for examining the memory of devices infected with malware, using SpyEye as an example. "Investigating Traces of Malware Infections Using Memory Forensics" (https://sect.iij.ad.jp/d/2011/12/194028.html) (in Japanese).

*48 Defined as DirectoryTableBase.

*49 Defined as _KDDEBUGGER_DATA64.

*50 IIJ has confirmed this phenomenon on x64 architecture Windows 7 devices equipped with 16 GB of memory. According to Matthieu Suiche, author of the after-mentioned DumpIt acquisition tool that incorporates its own logic to decode the debug structure, this phenomenon can occur in Vista and later OSes.

■ Testing of Acquisition Tools

Some acquisition tools decode the debug structure that is encoded at the time of acquisition. IIJ tested five acquisition tools, FTK Imager*51, Belkasoft Live RAM Capturer*52, Windows Memory Reader*53, winpmem*54, and DumpIt*55, and checked whether they decoded the debug structure. Table 1 shows the results of these tests.

From the results, we found that only the crash dump format image created by DumpIt included decoded debug structure data*56. Figure 12 shows a comparison of encoded and decoded debug structure data. The top image is encoded data acquired using FTK Imager, and the bottom image is decoded data acquired using DumpIt. In the decoded data, we can see the "KDBG" signature in the debug structure header*57, as well as information on the size of the debug structure.

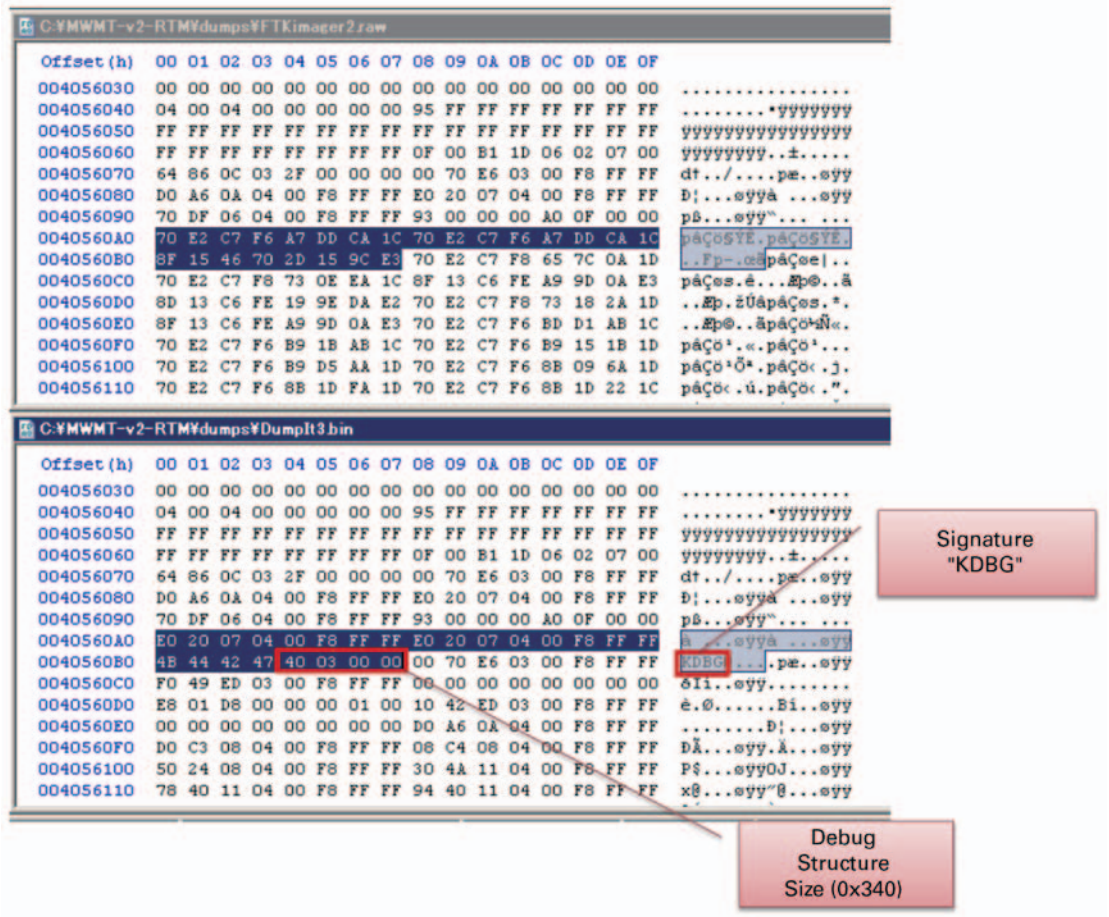


Figure 12: Debug Structure Data Comparison

*51 Version 3.1.4.6 used (http://www.accessdata.com/support/product-downloads).

*52 (http://forensic.belkasoft.com/en/ram-capturer).

*53 Version 1.0 used (http://cybermarshal.com/index.php/cyber-marshal-utilities/windows-memory-reader).

*54 Version 1.4.1 used (http://sourceforge.net/projects/volatility.mirror/files/?source=navbar).

*55 Version 2.0 used (http://www.moonsols.com/windows-memory-toolkit/).

*56 In IIJ's tests, of the tools listed, only the DumpIt crash dump format image included the decoded debug structure. However, the results may differ even if carried out using the same OS environment and tools. For example, the article below reports that it was possible to analyze memory images acquired using FTK Imager and Belkasoft RAMCapture (however, the writer does not appear to have confirmed that the debug structure was explicitly encoded, so it is possible the tools did not expressly perform decoding, and the debug structure was not encoded to begin with). This demonstrates that the criteria for the debug structure being encoded are not clear for OSes prior to Windows 7. BriMor Labs, "All memory dumping tools are not the same" (http://brimorlabs.blogspot.jp/2014/01/all-memory-dumping-tools-are-not-same.html).

*57 The header at the start of _KDDEBUGGER_DATA64, defined as _DBGKD_DEBUG_DATA_HEADER64

When the analysis tool used only supports raw formats, it is possible to use a workaround by converting a crash dump acquired using DumpIt to raw format. Incidentally, Windows Memory Reader and winpmem can create crash dump images. We previously mentioned that for crash dump images, the header at the start of the file contains the information required for analysis. That means tools that can directly analyze crash dump images without converting them should be able to return results even if the debug structure is encoded. However, some analysis tools still abort during analysis in the same way as for raw format images. Specifically, the Volatility Framework*58 implementation still searches for the debug structure even when a crash dump image is used, causing analysis to fail*59. CrashDumpAnalyzer*60 performs analysis using only the crash dump header information, so it can analyze crash dump images (with the debug structure encoded) created using Windows Memory Reader and winpmem.

■ Summary

As explained above, although at first glance the acquisition and analysis tools for memory forensics appear to acquire and analyze the same file formats, their implementations differ greatly. Analysts must have sufficient understanding of the characteristics of these tools when using them, or it may not be possible to extract volatile information through memory forensics at all, as demonstrated by the phenomenon discussed here. It is important to test tools on a regular basis, gather information from a wide range of sources, and investigate the cause of issues thoroughly, rather than overlooking them when they occur.

1.4.2 Forward Secrecy

In this section we discuss forward secrecy, which has come into the spotlight due to a series of news reports regarding the NSA. SSL/TLS server support for forward secrecy was introduced at major sites such as SNS at the end of last year. Below we examine the reasons forward secrecy was recognized as being necessary, provide a technical explanation, and discuss points to note when applying it.

■ Reasons Forward Secrecy was Recognized as Necessary

Recently, (perfect) forward secrecy*61 has garnered a lot of attention, but the concept has existed since at least an article presented at EUROCRYPT '89*62. We will not go into its cryptographic definition here, but it involves the generation of temporary key pairs used only for a single session via a procedure that uses key exchange protocols such as Diffie-Hellman*63. Even if the private key for this temporary public key is leaked, it is possible to limit the scope of encrypted communications disclosed.

Meanwhile, in cases where communications are encrypted using the same public key each time, if the encrypted data is propagated over a wide-area network, encrypted communications will continue to be stored over an extended period of decades. That means that if the private key is leaked at some point in the future, retrospective decryption is possible. Forward secrecy has drawn attention as a technique for preventing this issue.

*58 An open source memory analysis tool written in Python. It supports all raw, crash dump, and hibernation image formats. Because Volatility uses a generator that always searches for the debug structure regardless of format when listing the process structure, analysis fails when the debug structure is encoded. (https://code.google.com/p/volatility/).

*59 According to the following article, Volatility Framework has implemented experimental code for decoding the debug structure during analysis, and this is scheduled to be distributed to training participants. It states that the phenomenon of the debug structure being encoded can occur in new OSes such as Windows 8 and Server 2012 regardless of memory size. Volatility Labs, "The Secret to 64-bit Windows 8 and 2012 Raw Memory Dump Forensics" (http://volatility-labs.blogspot.jp/2014/01/the-secret-to-64-bit-windows-8-and-2012.html).

*60 A crash dump analysis tool written in the EnScript scripting extension language for EnCase. The information that can be extracted is limited compared to Volatility. (http://takahiroharuyama.github.io/blog/2014/01/05/some-old-stuffs/).

*61 The terms "perfect forward secrecy" and "forward secrecy" are both used interchangeably, so we have unified this as "forward secrecy" in this document.

*62 Christoph G. Günther, "An Identity-Based Key-Exchange Protocol", EUROCRYPT1989, LNCS vol.434, pp.29-37, 1989.

*63 The Diffie-Hellman key exchange method is generally described as follows. Generator g for the finite field GF(p) of sufficiently large prime p is set, and p and g are made public parameters (they do not need to be kept secret). User A and User B select random private keys x and y from integers between 1 and p-1, and $X=g^x \bmod p$ and $Y=g^y \bmod p$ are reciprocally disclosed as the public keys for User A and User B. User A can calculate $Y^x = (g^y)^x \bmod p$ using User B's public key Y. Meanwhile, User B can calculate $X^y = (g^x)^y \bmod p$ using User A's public key X, so $g^{xy} \bmod p$ can be shared in secret by User A and B alone. The discrete logarithm problem for finding x from g, g^x, and p is considered difficult when using a sufficiently large prime p.

Forward secrecy started attracting attention after a series of news reports regarding the National Security Agency (NSA) interception of communications. Last September, it was reported that part of a cryptographic algorithm designed by the National Institute of Standards and Technology (NIST) contained an NSA backdoor that made decrypting possible. NIST published a statement denying they had intentionally adopted weak cryptography, and recommended against use of the Dual_EC_DRBG pseudo-random number generation algorithm*64. This news was also publicized by CRYPTREC in Japan*65. In response, U.S. EMC told customers of its RSA BSAFE cryptographic library which is configured to use Dual_EC_DRBG by default, not to use this algorithm*66. Reports on EMC and the NSA were also made subsequently. A vulnerability in Dual_EC_DRBG that made it possible to identify the random number sequence if 32 bytes of the pseudo-random number output were obtained was already disclosed in 2007*67. Although this kind of issue was uncovered, it continued to be used where cryptographic algorithms were applied.

This could lead to attackers stealing information in real-time, such as all pseudo-random number used during communications, as well as encryption keys generated from them, by placing a pseudo-random number generator module under their control. In fact, problems resulting from the low entropy of pseudo-random number generator modules are already known, including an OpenSSL vulnerability in Debian*68. This vulnerability involved an issue with private keys being derived only from a greatly reduced key space when generating key pairs using OpenSSL in certain versions of Debian. Although this issue was pointed out in 2008, sites using these vulnerable keys still exist now. Problems occurring during random number generation in some Bitcoin applications on Android have also been reported*69. A random number parameter must be generated each time signing is carried out for the ECDSA signatures used in Bitcoin. If the same parameter is used for generation of different signatures, the private key is revealed. This is another issue caused by the low entropy of pseudo-random number generators.

Other NSA mechanisms for intercepting communications in addition to placing backdoors in cryptographic algorithms are also coming out into the open. Last June it was reported that the NSA had asked U.S. Verizon to gather phone call logs. It was also revealed that the PRISM program for collecting data such as videos, photos, and emails on the Internet was operating with the cooperation of major Internet-related companies in the U.S. Additionally, in October the existence of an NSA project for the real-time interception of communications was uncovered, and it came to light that communications between Yahoo! and Google data centers were being intercepted. The Lavabit email provider was also instructed by the FBI to hand over its private keys, and opted to shut down their service after deciding that they could no longer protect their users' privacy. Through specific cases like this, it is becoming clear that communications could be intercepted by the NSA or other organizations even when they are encrypted using secure protocols. At IETF-88, which was held last November, pervasive surveillance was addressed as one of the main topics*70*71*72. Forward secrecy has been taken up as a method for dealing with this.

*64 NIST, "SUPPLEMENTAL ITL BULLETIN FOR SEPTEMBER 2013" (http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf).

*65 CRYPTREC, Regarding the Dual_EC_DRBG pseudo-random number generator algorithm (http://www.cryptrec.go.jp/topics/cryptrec_20131106_dual_ec_drbg.html) (in Japanese).

*66 ArsTechica, "Stop using NSA-influenced code in our products, RSA tells customers" (http://arstechnica.com/security/2013/09/stop-using-nsa-influence-code-in-our-product-rsa-tells-customers/?comments=1&post=25330407#comment-25330407).

*67 Dan Shumow, Niels Ferguson, "On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng", Rump session in CRYPTO2007 (http://rump2007.cr.yp.to/15-shumow.pdf).

*68 Debian Security Advisory, "DSA-1571-1 openssl -- predictable random number generator" (http://www.debian.org/security/2008/dsa-1571). Similar incidents are discussed in IIR Vol.17, under "1.4.1 The Issue of Many Public Keys Used with SSL/TLS and SSH Sharing Private Keys with Other Sites" (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol17_EN.pdf).

*69 bitcoin.org, "Android Security Vulnerability" (http://bitcoin.org/en/alert/2013-08-11-android). Regarding this incident, actual damages were observed in the following paper. Joppe W. Bos, J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, Eric Wustrow, "Elliptic Curve Cryptography in Practice" (https://eprint.iacr.org/2013/734).

*70 IETF Blog, "We Will Strengthen the Internet" (http://www.ietf.org/blog/2013/11/we-will-strengthen-the-internet/).

*71 CA Security COUNCIL Blog, "IETF 88 - Pervasive Surveillance" (https://casecurity.org/2013/11/26/ietf-88-pervasive-surveillance/).

*72 "IETF 88 Technical Plenary: Hardening The Internet" (https://www.youtube.com/watch?v=oV71hhEpQ20).

An Overview of Forward Secrecy

The issue mentioned above has already been recognized in the field of content security, as it affects areas such as storage encryption. This is because encrypted data becomes a target for brute force attacks once it is released to third parties. In other words, when encrypted data is published, the corresponding data is in a state where it can be decrypted, and attackers can attempt to decrypt it using all the keys for common key cryptosystem such as AES. Meanwhile, signatures are standardized as long-term signatures, allowing verification over long periods of time by also signing the verification information for a certain point in time in conjunction with the time stamp. However, no long-term storage technology has been established for data encryption.

On the other hand, the concept of long-term signatures is not needed for secure communication protocols such as SSL/TLS, because there is no need to guarantee the long-term integrity of data flowing over secure channels established between clients and servers. However, as indicated above, a system for guaranteeing confidentiality is necessary, because encrypted communications may be compromised through being recorded continuously over decades. It is assumed that secure data storage may be decrypted in the distant future in some cases, so the keys used for encryption must be managed appropriately. Meanwhile, for temporarily encryption using secure communication protocols, there is no need to save the key used for encryption. This demonstrates that the perspective of cryptographic key management differs greatly. The idea of forward secrecy uses this contrasting characteristic of "temporarily used keys being disposable."

Generally, a hybrid method using both the common key cryptosystem and the public key cryptosystem is used for secure communication protocols and secure data storage. Common key cryptosystems are used for actual data encryption, and the content key (the key used to encrypt data) is encrypted with a public key cryptosystem. One example of this is the procedure of encrypting the content key used in the AES algorithm with an RSA public key.

For SSL/TLS, key exchange algorithms such as RSA, DH_RSA, and DHE_RSA are prescribed. Key exchange algorithms are used to securely exchange the source data for deriving content keys or MAC keys. For example, when the RSA is selected as the key exchange algorithm, the premaster secret is securely exchanged. The premaster secret is random data created by the client, and can be securely exchanged with a server by encrypting it using the public key stored in the server certificate. In other words, the RSA algorithm is used for both server authentication and key exchange. For DH_RSA, secure data exchange is carried out via the DH key exchange algorithm using the DH public key included in the certificate. Meanwhile, with DHE_RSA, a temporary DH public key and private key that change each time are generated*73.

Here we will consider a case in which the private key corresponding to a public key listed in a server certificate leaked at a later date. When the RSA or DH_RSA key exchange algorithm is used, if encrypted communications have been intercepted over a long period of time, the content key can be derived from these records because key exchange is carried out using a fixed public key. This means that the content of communications at that point is divulged from the encrypted communication data.

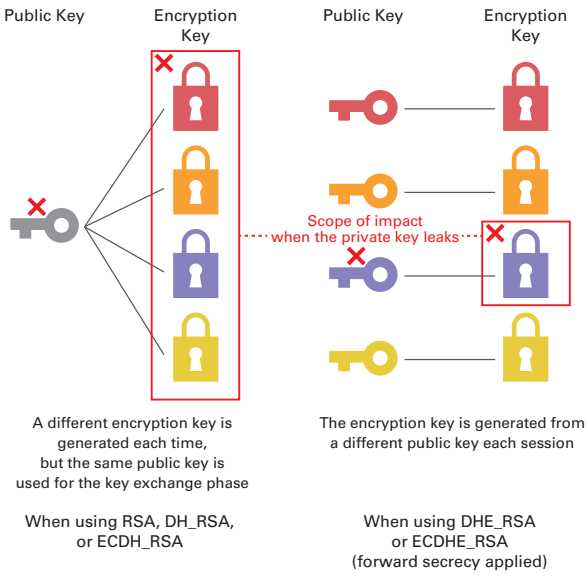


Figure 13: Differences between Not Applying / Applying Forward Secrecy in TLS

*73 The E in "DHE_*" stands for "ephemeral." The structure of ServerDHParams described in RFC is designed to enable the storage and sending of the prime p of up to 2^{16} bits in length, the generator g, and the public key $Y=g^y$ (y is the private key).

Meanwhile, for DHE_RSA, a DH public key and a DH private key are generated for each session and discarded afterwards. This means that to decrypt encrypted communications data, the DH private key used for the communications must be revealed. Even if the DH private key is revealed, only communications encrypted with the content key derived securely using the corresponding DH public key is divulged, making it possible to limit the scope of damage. Figure 13 maps out the public keys used to derive encryptions keys. It could also be said that this maps out the encryption keys divulged when the private key corresponding to a public key is revealed. Use of DHE_RSA means conducting encrypted communications by creating disposable public keys as needed. At this time, the temporarily generated DH public key is secured using an RSA certificate on the server, preventing the weakness against MITM attacks that the DH key exchange algorithm potentially has.

For TLS, a cipher suite that can enable forward secrecy has been established since RFC2246 (TLS1.0), which was drawn up in 1999*74. Recently, a variant of DH using elliptic curve cryptography called ECDH has also been used*75. ECDH has been available since RFC4492, which was developed in 2006. Key exchange algorithms that support forward secrecy are described as "ECDHE_*"*76. ECDH generally enables faster processing than DH, so use of ECDH is spreading on a variety of clients and servers.

■ Forward Secrecy Application Examples and Points to Note

Starting with Google*77, which introduced support for forward secrecy in 2011, other companies including Facebook*78, Twitter*79, and GitHub*80 announced support or planned support in 2013. The EFF (Electronic Frontier Foundation) also provides frequent updates on the support status of major sites*81. In response to this growing support, specific configuration examples for Apache+SSL, etc., have also been put together for engineers*82. However, even when forward secrecy is enabled, it is not possible to completely prevent pervasive surveillance. Below we touch upon the issues that cannot be avoided even when forward secrecy is used.

First, we will discuss the underlying problems with (EC)DH key exchange algorithms. When an RSA private key leaks through a server compromise, etc., or when the RSA algorithm itself is compromised, subsequent encrypted communications may leak even when forward secrecy is enabled and disposable public keys are used. For example, let us examine a case in which DHE_RSA is used as the key exchange algorithm for TLS. Clients confirm the legitimacy of the temporary DH public key sent from the server, but because attackers inserting themselves between client and server have the RSA private key, they can rewrite the DH public key sent from the server, enabling MITM attacks. For this reason, when an RSA key is compromised, subsequent encrypted communications can be decrypted. In this case, it is possible to deal with the issue by updating the RSA key pair and the server certificate.

Next, we will take a look at issues with pseudo-random number generator modules. In the new e-Government Recommended Ciphers List revised in 2013, the pseudo-random number generator algorithm category has been deleted, and it will be necessary to rethink which pseudo-random numbers should be used in e-government systems and private sector information systems. There were guidelines regarding the use of pseudo-random number generator algorithms corresponding to the old

*74 The TLS Protocol Version 1.0 (http://www.ietf.org/rfc/rfc2246.txt).

*75 Specific algorithms are listed in "Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" (http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf) under section 5.7.1. Like DH, security is based on the discrete logarithm problem on an elliptic curve.

*76 Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) (http://www.ietf.org/rfc/rfc4492.txt).

*77 Google Online Security Blog, "Protecting data for the long term with forward secrecy" (http://googleonlinesecurity.blogspot.jp/2011/11/protecting-data-for-long-term-with.html).

*78 Facebook Engineering, "Secure browsing by default" (https://www.facebook.com/notes/facebook-engineering/secure-browsing-by-default/10151590414803920).

*79 The Twitter Engineering Blog, "Forward Secrecy at Twitter" (https://blog.twitter.com/2013/forward-secrecy-at-twitter-0).

*80 The GitHub Blog, "Introducing Forward Secrecy and Authenticated Encryption Ciphers" (https://github.com/blog/1727-introducing-forward-secrecy-and-authenticated-encryption-ciphers).

*81 Electronic Frontier Foundation, "UPDATE: Encrypt the Web Report: Who's Doing What" (https://www.eff.org/deeplinks/2013/11/encrypt-web-report-whos-doing-what#crypto-chart).

*82 Qualys Community, "Configuring Apache, Nginx, and OpenSSL for Forward Secrecy" (https://community.qualys.com/blogs/securitylabs/2013/08/05/configuring-apache-nginx-and-openssl-for-forward-secrecy). Because some cipher suites can only be used with TLS1.1 or TLS1.2, they depend on the support status for cryptographic algorithms such as OpenSSL. For example, for OpenSSL, library version 1.0.0h and later support TLS1.2. It should also be noted that OpenSSL has adopted a different description method than the cipher suite described in the RFC (http://www.openssl.org/docs/apps/ciphers.html#CIPHER_SUITE_NAMES).

version of the list, but these have not been updated, and now they cannot be considered valid*83. We believe that the pseudo-random number generator algorithm category was deleted because it does not require compatibility to be secured. However, even with it deleted from the list, guidelines regarding points to note when using/implementing would be appreciated.

In many cases, random number generator modules are used via cryptographic libraries. Validation programs for these cryptographic libraries include CMVP*84 and JCMVP*85, and it is believed that using these will enable libraries to be used securely. However, it has been revealed that there were issues with the previously-mentioned RSA BSAFE, despite it being a cryptographic library endorsed by government agencies. Even when the security of a cryptographic library has been confirmed, it is necessary to ensure that there are no issues with its usage, such as short seed or nonce values being input into the pseudo-random number generator module.

Figure 14 summarizes the phases in which pseudo-random number modules are used for the TLS protocol. Before using TLS, the server generates an RSA key pair and creates a server certificate. At that time, the server generates prime numbers using a pseudo-random number generator module, but as mentioned previously, as with the Debian OpenSSL issue, it is necessary to secure sufficient entropy. The TLS protocol begins by sending a "Hello" to both the client and server. A random value containing a 28-byte piece of random data is generated for the transmission of the ClientHello and ServerHello messages. Furthermore, when RSA is selected as the key exchange algorithm, a PreMasterSecret including a 46-byte piece of random data is shared securely via the ClientKeyExchange message. When using DHE or ECDHE, the PreMasterSecret is shared by generating a temporary DH key or ECDH key, and executing the key exchange algorithm. At this time, the risk of decryption is higher if the selection range for the temporary (EC)DH private key is small. Finally, the MasterSecret is calculated from three pieces of random data: ClientHello.random, ServerHello.random and PreMasterSecret. Secure communications can be carried out by deriving the MAC key, content key, and initial vector (IV) (when CBC mode is used) for both client and server from this MasterSecret. TLS is designed to derive the encryption key using a number of pieces of random data, but in cases where secure pseudo-random number generation isn't possible, or in other words when there is bias in the values generated, TLS may not be usable securely.

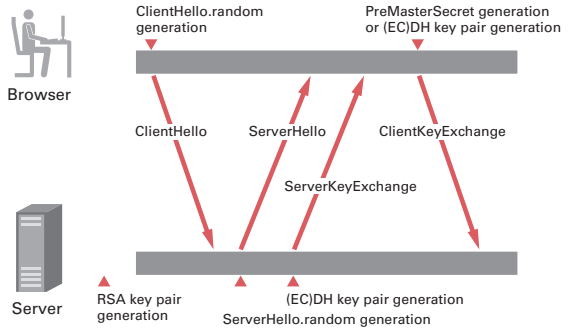


Figure 14: Timing of Using the Pseudo-Random Number Generator in TLS

1.4.3 Website Defacement Surveys Using Web Crawlers

As a part of our MITF (Malware Investigation Task Force) anti-malware activities, IIJ has been operating Web crawlers for surveying website defacements and collecting drive-by download malware specimens since 2008. In this section, we give an overview of the current Web crawler environment, and discuss trends in recent observations.

*83 The Guidebook for e-Government recommended ciphers (http://www.cryptrec.go.jp/report/c07_guide_final_v3.pdf) (in Japanese) lists having a generated value of sufficient length so that identical values are not generated, having no bias in the generated values, and having generated values that cannot be predicted as requirements for using a number of secure protocols. Chapter 6 of the list guide for 2009 (http://www.cryptrec.go.jp/report/c09_guide_final.pdf) (in Japanese) contains a section on pseudo-random number generators.

*84 The Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) is a system for testing cryptographic modules established by NIST.

*85 The Japan Cryptographic Module Validation Program (http://www.ipa.go.jp/security/jcmvp/) (in Japanese) is Japan's version of CMVP. It is operated by the Information-technology Promotion Agency, Japan. Joint validation for recognizing products validated by both JCMVP and CMVP has also been applied. (http://www.ipa.go.jp/about/press/20120227.html) (in Japanese).

■ A Surge in Web Defacements, and Web Crawlers

In June 2013, IPA and the National Police Agency published a warning regarding a rash of website defacements*86. According to a JPCERT/CC report, between October and December 2013, 2,774 Web defacements were reported*87.

Most recent incidents of website defacement have not been crimes committed out of fun or as political offenses with the intention of overwriting content. Instead, the majority have been attempts to redirect visitors to malware distribution sites by inserting elements such as iframe tags into content. These types of Web defacement have become increasingly widespread both inside and outside Japan since the Gumblar incident*88 in 2008. Although these cases have been ongoing ever since, incidents in Japan increased markedly in 2013*89. In a number of incidents, well-known and popular sites generally thought to be secure have been defaced, exposing large numbers of visitors to danger. In light of this situation, the MITF conducts surveys for identifying Web defacement trends to implement effective countermeasures.

The best way to survey whether a certain website has been defaced to infect visitors with malware, etc., is to build an environment capable of capturing communications and acquiring a list of sites accessed and their content, which can be restored to its original state easily once confirmation is complete. You would then actually launch a Web browser and view the site manually to test whether malware infection occurs. However, attempting to manually visit large numbers of websites every day and check for malware infections would require a vast amount of manual labor, so this is not realistic. MITF's Web crawler is a mechanism for automating tasks like this.

■ Client Honeypots and Their Types

The MITF Web crawler is a mechanism that crawls websites targeted for survey using a vulnerable client that will be infected by drive-by download*90 malware, or an environment that simulates a vulnerability. This is a system known as a client honeypot. When viewing websites defaced to carry out malware infections from this environment, it can collect defaced content, the files used in attacks, and malware that attackers intended to infect victims with.

Generally, client honeypots are broadly divided into two groups based on the method used to simulate actual environments.

1) High Interaction Client Honeypots
   A system equivalent to clients normally in use is prepared, such as a Windows environment. The target websites are viewed, and downloaded content is collected. Although this makes it possible to obtain accurate information almost identical to that when viewed using a standard client environment, there are downsides, such as it taking longer to crawl individual sites compared with low interaction client honeypots. Additionally, because actual malware infections occur, you have to go to the trouble of restoring the environment to its initial state each time. System building and operation are also very time-consuming (particularly when preparing multiple versions of a client environment).

2) Low Interaction Client Honeypots
   Content on the target websites is collected using tools for emulating client applications such as Web browsers. This method has the advantage of making it easy to build and operate systems, facilitating faster Web crawling, and not leading to actual malware infections because attack content is gathered by simply simulating vulnerabilities. However, it also has disadvantages. Specifically, it is unable to recreate the behavior of actual environments in some cases due to issues with the implementation of the JavaScript engine. Additionally, it is difficult to collect the payload downloaded as a result of attacks because it does not emulate all functions (vulnerabilities) attacked by drive-by downloads.

*86 IPA, "An alert for general users (website viewers) regarding an increase in website defacement" (http://www.ipa.go.jp/security/topics/alert20130626.html) (in Japanese) and "An alert regarding incidents such as website defacement - website defacements rising rapidly -" (http://www.ipa.go.jp/security/topics/alert20130906.html) (in Japanese), National Police Agency, "An alert regarding malware infections caused by viewing defaced websites" (http://www.npa.go.jp/cyberpolice/detect/pdf/20130626.pdf) (in Japanese).

*87 JPCERT/CC, JPCERT/CC Incident Report Response Report [October 1, 2013 to December 31, 2013]" (http://www.jpcert.or.jp/pr/2014/IR_Report20140116.pdf) (in Japanese).

*88 See "1.4.2 ID/Password Stealing Gumblar Malware" in Vol.4 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol04_EN.pdf) and "1.4.1 Renewed Gumblar Activity" in Vol.6 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol06_EN.pdf) for more information on Gumblar.

*89 See Vol.19 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol19_EN.pdf) under "1.4.2 Website Alterations and Drive-By Download Attacks in Japan" for more information about the website defacements that took place in Japan during March 2013.

*90 Drive-by downloads refer to the act of installing software (mainly malware) without a user's permission when Web content is viewed. They are often carried out by exploiting vulnerabilities in Web browsers and plug-ins.

IIJ has tested many implementations of these two types of client honeypots, but because there was no low interaction client honeypot implementation featuring enough functions from a reproducibility standpoint, we are currently building and operating our own high interaction client honeypots.

Detecting Drive-By Downloads by Identifying Redirection

After a client honeypot finishes crawling the Web, it is necessary to identify whether or not a drive-by download took place when viewing each site. However, the code inserted into Web content at the time of defacement and the payload downloaded when an attack succeeds are often changed frequently, so it is difficult to detect the latest attacks using signature-based mechanisms. Consequently, the MITF Web crawler uses a system that analyzes whether or not a drive-by download took place by extracting the superficial characteristics of communications that occur when a site is viewed. When it is determined that an attack took place, a more detailed analysis is carried out in a sandbox.

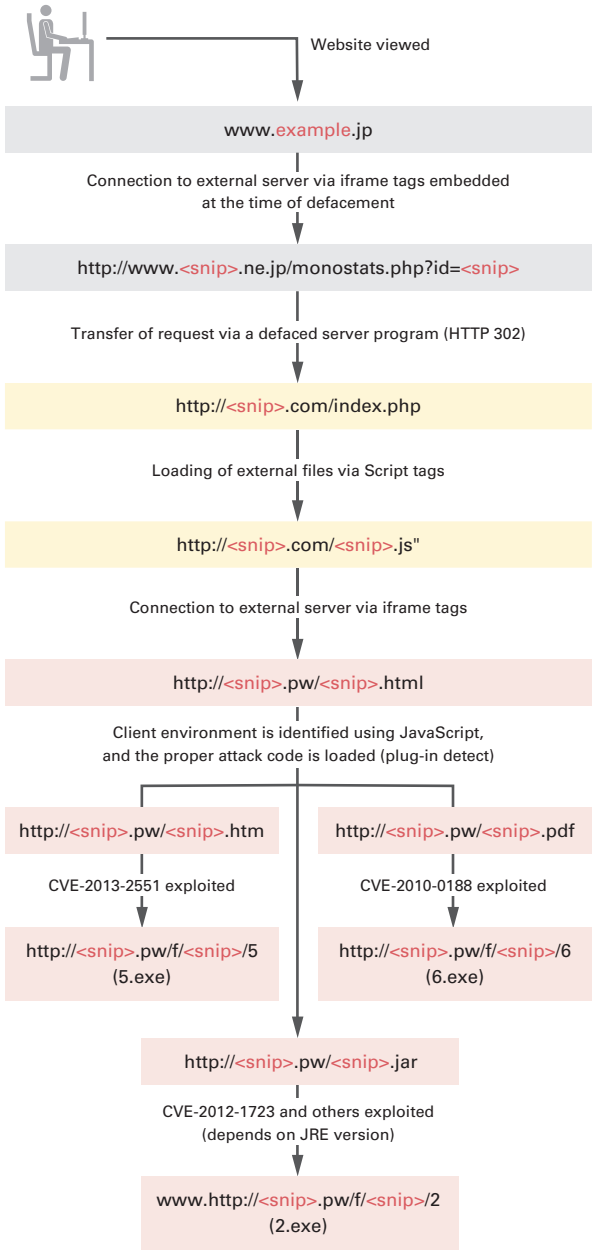
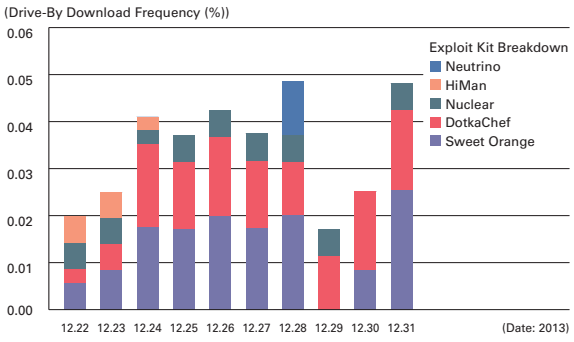


Figure 15: Sample Communications Flow When Viewing a Defaced Website

For example, Figure 15 shows typical connection transitions when a drive-by download occurs due to viewing a defaced website. The client is connected to three servers with domains different to www.example.jp, which the user initially intended to view. Content of types that are rarely loaded automatically during normal Web browsing, such as PDFs, Java (JAR), or Windows executables (EXE), are also acquired from these external domain servers. This means that it is possible to detect attacks comparatively quickly by identifying redirection outside a domain, and evaluating HTTP header information (content type, file size, User-Agent, etc.) at the time of communications with the redirection target based on drive-by download characteristic information configured in advance*91. Also, when it is determined that a corresponding website may have been defaced, system behavior at the time of viewing (APIs used, and details written to files and the registry, etc.) is automatically analyzed in a dynamic malware analysis environment, and precise information is logged regarding the presence of an attack as well as its details.



* Covers several tens of thousands of sites in Japan.
In recent years, drive-by downloads have been configured to change attack details and whether or not attacks are made based on the client system environment or session information, source address attributes, and the quota achievement status of factors such as number of attacks. This means that results can vary wildly at times depending on the test environment and circumstances.

Figure 16: Drive-By Download Frequency When Viewing Japanese Websites

*91 Because external content not placed intentionally by the operator is used on many websites, including mash-up content such as external tools and ads, white lists for these must also be configured.

■ Targeted Sites and Recent Observation Trends

The MITF Web crawler currently accesses tens of thousands of sites in Japan on a daily basis, focusing on well-known and popular sites. We also regularly add new target sites while adjusting the crawler's processing ability. In addition to this, we monitor websites that have seen short-term increases in access numbers on a temporary basis.

Figure 16 summarizes the observation results for December 22 to December 31, 2013. The vertical axis indicates the drive-by download frequency when viewing websites as a percentage, with the breakdown color-coded by the type of exploit kit used.

Sweet Orange or DotkaChef were used in many of the attacks observed during this period. From the exploits downloaded by the Web crawler, as well as the characteristics of these exploit kits*92, we estimate that vulnerabilities in JRE and IE were mainly targeted with regard to clients in Japan. Furthermore, from the characteristics of the URLs in defaced content, as well as the defaced content itself, we estimate that the defaced websites observed during this period involved the defacement of content files or server executable files after access authority for a legitimate server such as an FTP was stolen, or defacements exploiting an OpenX vulnerability*93 disclosed on December 18, 2013.

As this demonstrates, accessing a large number of websites and tallying up drive-by downloads enables us to identify fluctuations in the number of defaced sites, as well as trends in the vulnerabilities exploited, making it easier to evaluate the order of priority for preventative measures. We are continuing to make adjustments to the system, so we can publish trends we have observed such as those in this IIR on a regular basis. Regarding individual cases in which defacements were identified, we are looking into operational structures to enable us to provide reports and management support swiftly and efficiently to customers and related parties, as well as general Internet users in some cases. IIJ will continue to update our system in response to changes in circumstances and take appropriate measures to implement anti-malware activities.

1.5 Conclusion

This report has provided a summary of security incidents to which IIJ has responded. In this volume we discussed points to note regarding memory forensics for devices equipped with large amounts of memory. We also examined forward security, and summarized our surveys of website defacements using Web crawlers. IIJ makes every effort to inform the public about the dangers of Internet usage by identifying and publicizing incidents and associated responses in reports such as this. IIJ will continue striving to provide the necessary countermeasures to allow the safe and secure use of the Internet.

Authors:

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

Hirohide Tsuchiya (1.2 Incident Summary)
Hirohide Tsuchiya, Hiroshi Suzuki (1.3 Incident Survey)
Takahiro Haruyama (1.4.1 Points to Note Regarding Memory Forensics for Devices with Large Amounts of Memory)
Yuji Suga (1.4.2 Forward Secrecy)
Hisao Nashiwa (1.4.3 Website Defacement Surveys Using Web Crawlers)
Office of Emergency Response and Clearinghouse for Security Information, Service Operation Division, IIJ

Contributors:
Masahiko Kato, Masafumi Negishi, Tadashi Kobayashi, Yasunari Momoi
Office of Emergency Response and Clearinghouse for Security Information, Service Operation Division, IIJ

*92 A detailed overview of recently active exploit kits is summarized in "An Overview of Exploit Packs (Update 20) Jan 2014" (http://contagiodump.blogspot.jp/2010/06/overview-of-exploit-packs-update.html).
*93 "Zero Day Vulnerability in OpenX Source 2.8.11 and Revive Adserver 3.0.1" (http://www.kreativrauschen.com/blog/2013/12/18/zero-day-vulnerability-in-openx-source-2-8-11-and-revive-adserver-3-0-1/).