IIJ
Internet Initiative Japan

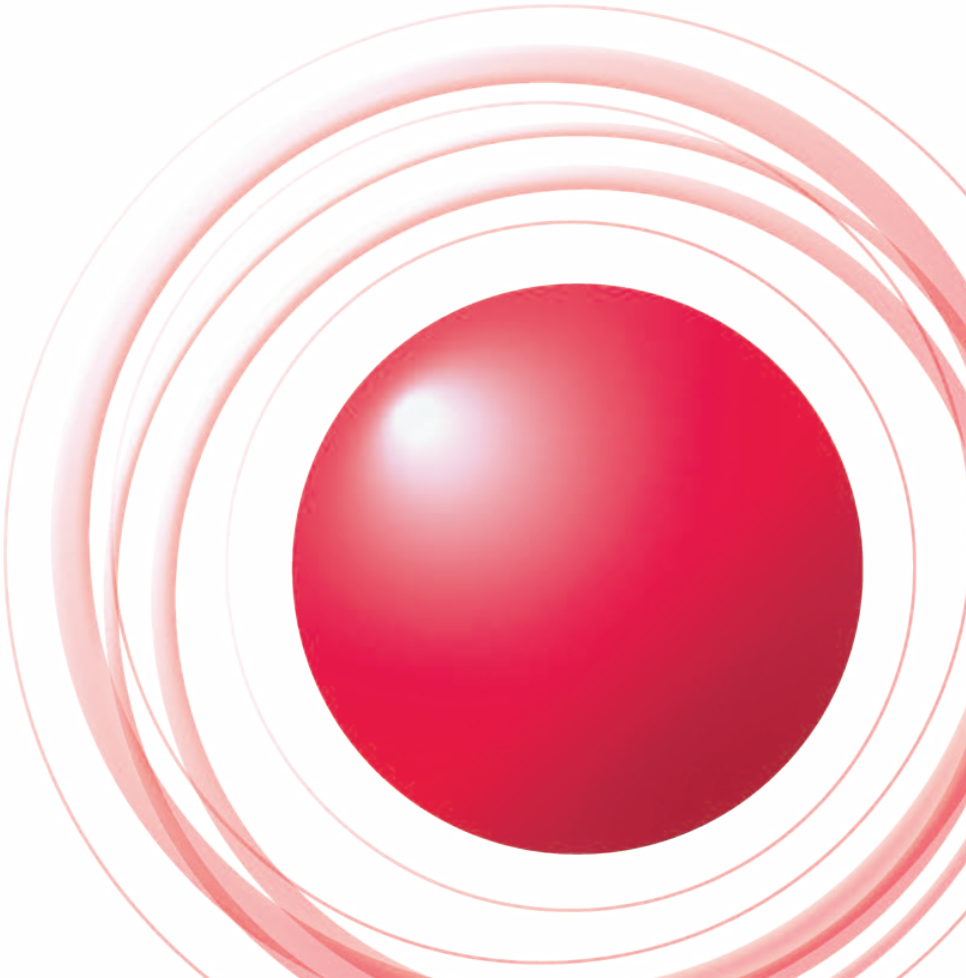
Internet Infrastructure Review Vol.27

May 2015

Infrastructure Security
Increasingly Malicious PUAs

Messaging Technology
Anti-Spam Measure Technology and DMARC Trends

Web Traffic Report
Report on Access Log Analysis Results for Streaming Delivery of the 2014 Summer Koshien



Internet Infrastructure Review

Vol.27 May 2015

■ To download current and past issues of the Internet Infrastructure Review in PDF format, please visit the IIJ website at http://www.iij.ad.jp/en/company/development/iir/.

Executive Summary

According to a report titled "Aggregation and Provisional Calculation of Internet Traffic in Japan," which was published by the Ministry of Internal Affairs and Communications on April 3, 2015, as of November 2014 the overall download traffic of broadband subscribers was estimated to be 3.6 Tbps. This is a 37.5% increase compared to the same month the previous year. The number of broadband subscribers remained almost flat during this period, showing only a slight increase, which means the shift towards users consuming larger-scale content is progressing.

Also, while the volume of mobile user download traffic was still comparatively small at 758 Gbps, it increased by 45.5%, which is higher than the overall increase rate. In the future it is likely that the growth of mobile traffic will be a driving factor in the growth of overall traffic volumes.

Meanwhile, major U.S. video streaming service Netflix has announced that it will launch a service in Japan this fall. It is thought that companies including Hulu and domestic operators such as acTVila and Hikari TV that have already entered the Japanese market will invest in their services to vie for customers, so the Internet-based online video streaming market is expected to see a major boost towards the latter half of this year. In the coming months there is likely to be a major upheaval in the state of Internet usage from a traffic perspective.

This report discusses the results of the various ongoing surveys and analysis activities that IIJ, as a service provider, carries out to support the Internet and cloud infrastructure, and enable our customers to continue to use them safely and securely. We also regularly present summaries of technological development as well as important technical information.

In the "Infrastructure Security" section, we give a month-by-month chronological summary of major incidents observed during the three months from January 1 to March 31, 2015, and report on the results of our statistics gathering and analyses for the entire period. We also present our focused research for this period, including a look at analysis results for PUA (Potentially Unwanted Programs) as well as discussion of the techniques used. In addition, we examine malware that reprograms HDD firmware, and continue our report on ID management technology from the previous volume.

In the "Messaging Technology" section, we report on our analysis of spam trends for the 52 weeks between March 31, 2014, and March 29, 2015, while also looking at long-term trends from IIR Vol.1 (June 2008). In our discussion of email technologies, we examine the DMARC technology for which an RFC was authored in March 2015, and discuss the creation of an environment for using it. In addition, we look at the email ecosystem, including domain reputation and feedback.

In the "Web Traffic Report" section, we analyze the logs of all delivery servers for the live streaming delivery of video for the National High School Baseball Championship at Koshien Stadium held in August 2014, which resulted in a peak traffic of 108 Gbps, and a total of approximately 1.9 billion requests. We also examine differences in access trends due to access scale and device type that were revealed through the results of this analysis.

Through activities such as these, IIJ continues to strive towards improving and developing our services on a daily basis while maintaining the stability of the Internet. We will keep providing a variety of solutions that our customers can take full advantage of as infrastructure for their corporate activities.

Author:

Toshiya Asaba
President and CEO, IIJ Innovation Institute Inc. President and CEO, Stratosphere Inc. Mr. Asaba joined IIJ in its inaugural year of 1992, becoming involved in backbone construction, route control, and interconnectivity with domestic and foreign ISPs. He was named IIJ director in 1999, and executive vice president in charge of technical development in 2004. When the IIJ Innovation Institute Inc. was founded in June 2008, Mr. Asaba became its president and CEO. When Stratosphere Inc. was founded in April 2012, he also became president and CEO of that organization.

Increasingly Malicious PUAs

In this report, we discuss increasingly malicious PUAs, and following on from our last report we cover actual usage cases for ID management technology, as well as initiatives for bolstering its security. We also look at the IOCs for malware that reprograms HDD firmware.

1.1 Introduction

This report summarizes incidents to which IIJ responded, based on general information obtained by IIJ itself related to the stable operation of the Internet, information from observations of incidents, information acquired through our services, and information obtained from companies and organizations with which IIJ has cooperative relationships. This volume covers the period of time from January 1 through March 31, 2015. In this period a number of hacktivism-based attacks were once again carried out by Anonymous and other groups, and there was a rash of attacks including SNS account hijackings and website defacements. There were also a large number of information leaks due to unauthorized access. It has been pointed out that the personal information of up to 80 million people may have leaked in an incident that occurred at a health insurer in the United States. An issue was also discovered in software pre-installed on PCs. This could potentially allow encrypted Web browser communications to be intercepted by a third party, or fraudulent websites to be recognized as legitimate. These examples show that many security-related incidents continue to occur on the Internet.

1.2 Incident Summary

Here, we discuss the IIJ handling and response to incidents that occurred between January 1 and March 31, 2015. Figure 1 shows the distribution of incidents handled during this period*1.

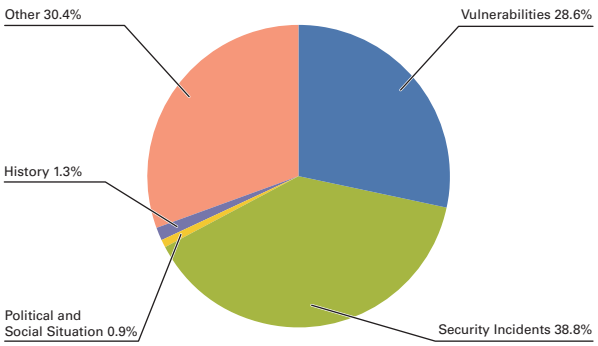


Figure 1: Incident Ratio by Category (January 1 to March 31, 2015)

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 corporate sites in a large number of countries stemming from a variety of situations and causes. In January, a number of Massachusetts Institute of Technology (MIT) websites were defaced in memory of an activist who committed suicide the year before last. Similarly, in the Philippines a number of government websites were defaced in protest against a firefight that took place between Police and an armed group on Mindanao Island in January. In February, DDoS attacks were made on multiple Saudi Arabian banks in protest against the Saudi

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

Arabian Royal Family (OpSaudi). SNS account hijackings by unknown attackers claiming affiliation with the Syrian Electronic Army also continued, with affected companies including French newspaper Le Monde. Other attacks by hacktivists such as Anonymous continued on government and government-related websites around the world. There were also ongoing hijacking incidents targeting the SNS accounts of government institutions and celebrities.

In addition, there have been a rash of attacks such as SNS account hijackings perpetrated worldwide by those claiming affiliation with ISIL or associated organizations. During the current survey period, in January there were incidents in which the official Twitter and YouTube accounts of the U.S. Central Command were hijacked, and the website of Malaysia Airlines was redirected to another website via DNS hijacking*2. Alterations to websites, including those for a number of companies in Japan, also garnered attention in March. These website alterations are thought to have been caused by attacks exploiting a WordPress plug-in vulnerability*3. Because attacks similar to these alteration incidents are occurring worldwide and not just in Japan, in April the FBI also issued an alert in the United States*4. In contrast, there were attacks thought to be carried out by Anonymous on Islamic extremist sites in response to a shooting at a weekly newspaper in France (OpCharlieHebdo), and attacks that resulted in the publishing of a list of ISIL-related accounts on SNS such as Twitter and Facebook, as well as account suspensions and the deletion of previous posts (OpISIS). There are also ongoing activities involving the publishing of lists of VPN and websites thought to be connected to ISIL and their hosting companies, with the intent of having them shut down or deleted.

■ Vulnerabilities and their Handling

During this period, fixes were released for Microsoft's Windows*5*6*7 and Internet Explorer*8*9. Fixes were also released for Adobe Systems' Adobe Flash Player. A quarterly update was provided for Oracle's Java SE, fixing many vulnerabilities. Several of these vulnerabilities were exploited in the wild before patches were released.

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 BIND9 DNS software that could cause abnormal operations or service outages on servers under specific conditions due to an issue with the management of DNSSEC trust anchors was fixed. A number of vulnerabilities that could allow the bypass of ACL rules or cause abnormal termination through the use of specially-crafted packets were fixed in the ntpd program used for time synchronization. A vulnerability that could cause the abnormal termination of applications through a buffer overflow was fixed in the GNU C Library (glibc) included in Linux distributions, etc. It was announced that there was also a vulnerability in SSL/TLS implementations that could allow encrypted information to be decrypted through MITM attacks exploiting implementations that accept weak RSA keys of 512 bits or less, which were used due to U.S. encryption export restrictions in the 1990s. This vulnerability was fixed in OpenSSL*10.

Google's Project Zero caused a stir when it announced it was possible to elevate privileges using DRAM errors caused by interference between memory cells when they are accessed due to the high density of cells (the rowhammer problem). A scheduled semiannual update for Cisco's IOS was also released, fixing a number of vulnerabilities that could lead to DoS attacks and memory leaks.

*2 Malaysia Airlines, "Media Statement on Malaysia Airlines' Website" (http://www.malaysiaairlines.com/my/en/corporate-info/press-room/2015/media-statement-malaysia-airlines-website.html).
*3 National Police Agency, "Alert regarding website defacements by those claiming affiliation with 'Islamic State (ISIS)'" (http://www.npa.go.jp/cyberpolice/detect/pdf/20150312.pdf) (in Japanese).
*4 The Internet Crime Complaint Center (IC3), "ISIL DEFACEMENTS EXPLOITING WORDPRESS VULNERABILITIES" (https://www.ic3.gov/media/2015/150407-1.aspx).
*5 "Microsoft Security Bulletin MS15-002 - Critical: Vulnerability in Windows Telnet Service Could Allow Remote Code Execution (3020393)" (https://technet.microsoft.com/library/security/ms15-002).
*6 "Microsoft Security Bulletin MS15-010 - Critical: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code Execution (3036220)" (https://technet.microsoft.com/library/security/ms15-010).
*7 "Microsoft Security Bulletin MS15-011 - Critical: Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)" (https://technet.microsoft.com/library/security/ms15-011).
*8 "Microsoft Security Bulletin MS15-009 - Critical: Security Update for Internet Explorer (3034682)" (https://technet.microsoft.com/library/security/ms15-009).
*9 "Microsoft Security Bulletin MS15-018 - Critical: Cumulative Security Update for Internet Explorer (3032359)" (https://technet.microsoft.com/library/security/ms15-018).
*10 "OpenSSL Security Advisory [08 Jan 2015] DTLS segmentation fault in dtls1_get_record (CVE-2014-3571)" (https://www.openssl.org/news/secadv_20150108.txt).

January Incidents

1 **S** **1st:** A number of incidents occurred in which malware was distributed via an ad distribution system used on news sites in Canada and the U.S.
Details can be found in the following Cyphort blog post. "HuffingtonPost Serving Malware via AOL Ad-Network" (http://www.cyphort.com/huffingtonpost-serving-malware/).

2 **V** **9th:** A number of vulnerabilities in OpenSSL that could cause service outages or allow arbitrary code execution were discovered and fixed.
"DTLS segmentation fault in dtls1_get_record (CVE-2014-3571)" (https://www.openssl.org/news/secadv_20150108.txt).

3 **O** **9th:** Microsoft announced they would no longer give an overview of their scheduled monthly security update program in advance via blog posts and the Web.
"Evolving Microsoft's Advance Notification Service in 2015" (http://blogs.technet.com/b/msrc/archive/2015/01/08/evolving-advance-notification-service-ans-in-2015.aspx).

4 **O** **9th:** The Japanese government established a Cyber Security Strategic Headquarters based on the enactment of the Bill on Cyber Security. They also set up the National center of Incident readiness and Strategy for Cybersecurity, a renaming of the National Information Security Center, as an organization to serve as the government's command post for cyber security.
"Regarding establishment of the National center of Incident readiness and Strategy for Cybersecurity" (http://www.nisc.go.jp/press/pdf/reorganization.pdf) (in Japanese).

5 **O** **12th:** President Obama announced a number of legislative proposals aimed at increasing protection of personal information, such as a requirement that companies notify their customers of information leaks within 30 days of them being discovered.
Whitehouse.gov, "FACT SHEET: Safeguarding American Consumers & Families" (https://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families).

6 **S** **13th:** An unknown party hijacked the Twitter (@CENTCOM) and YouTube accounts of the U.S. Central Command, and released a number of files said to contain classified information.
It was later confirmed that the information in the released files was publically available. U.S. Central Command, "Statement from U.S. Central Command Regarding Twitter/YouTube Compromise" (http://www.centcom.mil/en/news/articles/statement-from-u.s.-central-command-regarding-twitter-youtube-compromise).

7 **V** **14th:** Microsoft published their Security Bulletin Summary for January 2015, and released eight updates, including one critical update for MS15-002, as well as seven important updates.
"Microsoft Security Bulletin Summary for January 2015" (https://technet.microsoft.com/library/security/ms15-jan).

8 **V** **14th:** A number of vulnerabilities in Adobe Flash Player that could allow arbitrary code execution were discovered and fixed.
"Security updates available for Adobe Flash Player" (http://helpx.adobe.com/security/products/flash-player/apsb15-01.html).

9 **S** **19th:** Tokyo Metropolitan University announced that the NAS used on its campus had been accessible from outside via FTP connection, potentially exposing the personal information stored within.
"Regarding external access to NAS containing personal information at Tokyo Metropolitan University" (http://www.tmu.ac.jp/news/topics/8448.html?d=assets/files/download/news/press_150119.pdf) (in Japanese).

10 **O** **19th:** ENISA published a collection of information covering formats, standards, and tools for sharing threat information between organizations.
"Standards and tools for exchange and processing of actionable information" (https://www.enisa.europa.eu/activities/cert/support/actionable-information/standards-and-tools-for-exchange-and-processing-of-actionable-information).

11 **V** **21st:** Oracle released their quarterly scheduled update for a number of products including Oracle, fixing a total of 169 vulnerabilities, including 19 in Java SE. Additionally, because support for Java 7 ended in April 2015, measures were taken to automatically update to Java 8 in cases where the auto update function was enabled.
"Oracle Critical Patch Update Advisory - January 2015" (http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html).

12 **O** **21st:** The FBI issued a warning due to an increase in the damages caused by ransomware such as Cryptolocker and CryptWall.
FBI, "Ransomware on the RiseFBI and Partners Working to Combat This Cyber Threat" (http://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise).

13 **V** **23rd:** A vulnerability in a number of ASUSTeK brand wireless LAN routers that could allow unintended actions to be carried out through cross-site request forgery or OS command injection when a malicious website is viewed while logged in to the management screen was discovered and fixed.
"Request to update to firmware that fixes a cross-site request forgery and OS command injection vulnerability in wireless LAN router products (http://www.asus.com/jp/News/PNzPd7vkXtrKWXHR) (in Japanese).

14 **V** **23rd:** A vulnerability in Adobe Flash Player that could allow arbitrary code execution was discovered and fixed.
"APSB15-02: Security updates available for Adobe Flash Player" (http://helpx.adobe.com/security/products/flash-player/apsb15-02.html).

15 **O** **23rd:** The Telecom Information Sharing and Analysis Center Japan held an exercise that anticipated a large-scale cyber attack on communications infrastructure, with 12 organizations including member ISPs and critical infrastructure providers participating.
"Exercise for anticipating a cyber attack on communications infrastructure [CAE2015: Cyber Attack Exercise]" (https://www.telecom-isac.jp/news/news20150120.html) (in Japanese).

16 **V** **25th:** A vulnerability in Adobe Flash Player that could allow arbitrary code execution was discovered and fixed.
"APSB15-03: Security updates available for Adobe Flash Player" (https://helpx.adobe.com/security/products/flash-player/apsb15-03.html).

17 **V** **26th:** A vulnerability was found in wired LAN routers sold in 2004 that could lead to them being used as stepping stones in SSDP reflection attacks, and information on disabling the UPnP function in settings as a countermeasure was released.
JVN, "JVN#27142693 NP-BBRM vulnerable in UPnP functionality" (http://jvn.jp/en/jp/JVN27142693/).

18 **V** **28th:** A vulnerability in the glibc library that could cause service outages or allow remote arbitrary remote code execution through a buffer overflow was discovered and fixed.
"Qualys Security Advisory CVE-2015-0235 GHOST: glibc gethostbyname buffer overflow" (https://www.qualys.com/research/security-advisories/GHOST-CVE-2015-0235.txt).

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

*Dates are in Japan Standard Time

■ Attacks Targeting Home Routers

During the current survey period, a number of vulnerabilities in home routers were discovered and fixed. Several of these vulnerabilities could have allowed a third party to gain administrator privileges for the router without authorization, or change settings arbitrarily. Vulnerabilities that could allow a router to be exploited as a stepping stone in DrDoS attacks*11 were also discovered and fixed. Past attacks targeting home routers that exploited vulnerabilities include incidents that occurred in Brazil and other countries in 2011. In these incidents, router DNS settings were rewritten so that DNS servers prepared by the attacker were referenced, redirecting users to fraudulent sites*12. Similar attacks have also taken place more recently. For example, in March there were reports of an incident in which ads were distributed by exploiting the URL for a Web access analysis service*13. In Japan, there was an incident in which a provider was arrested for operating a proxy server used for unauthorized access in 2014. In this incident, it is thought that a vulnerability in home routers that was fixed in 2012 was exploited to obtain PPPoE authentication IDs and passwords unlawfully.

Unlike PCs, which are updated regularly, users tend to neglect to check the settings for home routers and update the firmware once they are set up. Consequently, even when a vulnerability is fixed, it may remain unpatched for a long time afterwards. It is expected that attacks targeting network devices such as home routers that are not managed properly in this way will continue to occur in the future. That means it will be necessary to manage these devices appropriately by confirming settings regularly and checking whether updated firmware has been released.

■ Unauthorized Login Through Identity Fraud

Since last year there have been many attempts to steal user IDs and passwords, and log in without authorization presumably using lists of these IDs and passwords. These attempts continued in the current survey period. Attacks have targeted a variety of websites, such as loyalty program sites, newspaper-related sites, and ISP support sites. In some cases these attacks resulted in monetary damages, such as the exchange of reward points without authorization.

■ Information Leaks Due to Unauthorized Access

Information leaks caused by unauthorized access also continue to occur. In January the website of a professional sports association in Japan was compromised, resulting in the leak of approximately 20,000 pieces of internal photo data. In February, there was an incident in which information on up to 80 million people, including past and present customers and employees, leaked from a U.S. health insurer after its internal database was accessed without authorization. In March, ICANN (Internet Corporation for Assigned Names and Numbers) was once again compromised, leading to suspension of the new gTLD system. Furthermore, in February there was an incident of unauthorized access at a domain registrar in Japan, causing damages such as the leak of the administrator information registered at the time of domain registration. In this incident, the company affected announced it would not resume service due to it being difficult to carry out in a timely manner, and they instead prompted customers to transfer domains to other operators*14. During the current survey period there were also malware infections and associated information leaks at a number of companies, including a trading company and a newspaper publisher. In these incidents, it was announced there were traces of client information and email content being sent to external parties from PCs infected through fraudulent email, which misrepresented the sender and had malware attached.

■ Government Agency Initiatives

Government agency initiatives included the January enforcement of the Act on Cyber Security that was passed last year, and the establishment of the Cyber Security Strategic Headquarters. The National Information Security Center was also reorganized into the National center of Incident readiness and Strategy for Cybersecurity. Additionally, the first general meeting of the Cyber Security Strategic Headquarters was held in February. At this meeting, new cyber security strategy for determining the details of future activities and basic policy for cyber security measures was discussed. In March, a bill to amend the Act on the Protection of Personal Information was approved by the Japanese cabinet. This bill is aimed at protecting personal information while also enabling the creation of new industries and services through promoting the

*11 See "1.4.2 DrDoS Attacks and Countermeasures" in Vol.23 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol23_EN.pdf) for more information.

*12 For more information, see the following IIJ-SECT blog post, "Home Routers Reference Fake DNS Server due to Unauthorized Configuration Changes" (https://sect.iij.ad.jp/d/2012/06/148528.html) (in Japanese).

*13 Ara Labs Technology, "Ad-Fraud Malware Hijacks Router DNS – Injects Ads Via Google Analytics" (http://aralabs.com/2015/03/25/ad-fraud-malware-hijacks-router-dns-injects-ads-via-google-analytics/).

*14 Telework Communications Co., Ltd., "Apology and report regarding the leak of customer information" (http://www.ariqui.net/) (in Japanese).

February Incidents

1 **1st:** A researcher at a security company in the U.K. announced there was a universal cross-site scripting (XSS) vulnerability with no fix available in Microsoft's Internet Explorer 11.

2 **2nd:** A large-scale DoS attack targeting a specific domain took place over a number of days, causing outages on multiple DNS servers in Japan.

3

4 **4th:** Vulnerabilities in ntpd were discovered and fixed. These could allow the bypass of ACL rules via IP address spoofing (CVE-2014-9298), or cause information leaks and abnormal termination through the use of specially-crafted packets (CVE-2014-9297).
US-CERT, "Vulnerability Note VU#852879 NTP Project Network Time Protocol daemon (ntpd) contains multiple vulnerabilities (Updated)" (http://www.kb.cert.org/vuls/id/852879).

5

6 **4th:** The man suspected of being behind the Remote Control Virus incident in 2013 received a prison sentence of eight years.

7

8 **5th:** U.S. health insurer Anthem announced a database containing information on around 80 million current and former customers and employees had been compromised.
Anthem, "How to Access & Sign Up For Identity Theft Repair & Credit Monitoring Services" (https://www.anthemfacts.com/).

9

10 **6th:** A number of vulnerabilities in Adobe Flash Player that could allow arbitrary code execution were discovered and fixed.
"APSB15-04: Security updates available for Adobe Flash Player" (https://helpx.adobe.com/security/products/flash-player/apsb15-04.html).

11 **6th:** IPA published "10 Major Security Threats for the Year 2015."
"10 Major Security Threats for the Year 2015." (https://www.ipa.go.jp/security/vuln/10threats2015.html) (in Japanese).

12

13 **10th:** The Japanese government held the 1st general meeting of the Cyber Security Strategic Headquarters, where discussions were held regarding establishing cyber security strategies for the comprehensive and effective promotion of cyber security measures.
"1st General Meeting (February 10, 2015)" (http://www.nisc.go.jp/conference/cs/index.html#cs01) (in Japanese).

14

15 **11th:** Microsoft published their Security Bulletin Summary for February 2015, and released nine updates, including three critical updates for MS15-009, MS15-010, and MS15-011, as well as six important updates.
"Microsoft Security Bulletin Summary for February 2015" (https://technet.microsoft.com/library/security/ms15-feb).

16

17

18 **13th:** In the United States, an executive order calling for information sharing between government agencies and private-sector businesses to protect against cyberspace threats and system breaches came into effect.
Whitehouse.gov, "FACT SHEET: Executive Order Promoting Private Sector Cybersecurity Information Sharing" (https://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform).

19

20 **18th:** Microsoft announced it had established a Japan satellite of its Cybercrime Center for researching cybercrime countermeasures, and indicated that it intended to provide information and technical support to customers including government agencies and companies.
"'Microsoft Cybercrime Center - Japan Satellite' established to reinforce cyber security initiatives in Japan" (http://news.microsoft.com/ja-jp/2015/02/18/150218-cybercrimecenter-japan/) (in Japanese).

21

22

23 **19th:** A vulnerability was discovered and fixed in BIND9. This vulnerability could cause abnormal operations or service outages on servers due to an issue with the implementation of exception handling for the auto update of trust anchors.
Internet Systems Consortium, "CVE-2015-1349: A Problem with Trust Anchor Management Can Cause named to Crash" (https://kb.isc.org/article/AA-01235).

24

25 **20th:** A number of issues were discovered and fixed in software pre-installed on PCs that could allow MITM attacks or fake websites with falsified certificates.
See the following Lenovo announcement for more information about this incident. "SuperFish Vulnerability" (http://support.lenovo.com/us/en/product_security/superfish).

26

27 **20th:** The Information Technology Promotion Agency, Japan (IPA) issued an alert regarding problems with unintended information leaks through the use of Web services, such as information that users enter into a translation service website being published on the Internet.
"Press Release [Alert] Beware of unintended information leaks regarding data entered into cloud services" (http://www.ipa.go.jp/about/press/20150220.html) (in Japanese).

28

25th: Europol's European Cybercrime Center (EC3) announced that the Ramnit botnet had been taken down in a joint operation with a number of security vendors such as Microsoft and Symantec.
"Botnet taken down through international law enforcement cooperation" (https://www.europol.europa.eu/content/botnet-taken-down-through-international-law-enforcement-cooperation).

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

*Dates are in Japan Standard Time

utilization of personal data, and improving the safety and security of citizens. To contribute to the protection and utility of personal information, the bill defines personal information more clearly, and establishes rules regarding the handling of data that is anonymized and cannot be reconstructed into personal information. It also prescribes the creation of a third-party Personal Information Protection Committee with authority to monitor and supervise the handling of personal information. Furthermore, in response to information leaks, penalties for the unauthorized supply or theft of data from a database containing personal information were increased, including the establishment of the Crime of Supplying Personal Information Databases. This cabinet decision also included an amendment to the systems for promoting the use of specific personal information (information including personal identity numbers), expanding the scope of usage for personal identity numbers in fields such as finance and health care.

■ Issues with Software Pre-Installed on PCs

During this survey period, issues with software preinstalled on Lenovo PCs received widespread attention. This software, which was installed on PCs shipped between September 2014 and January 2015 when this practice stopped, was so-called adware, and contained functions for inserting and displaying ads in a user's browser screen. One particularly problematic behavior it exhibited was that it could even insert ads into encrypted SSL/TLS communications, because it installed self-signed certificates to the local certificate store. A number of other issues were also identified, such as the fact that the encryption method for these installed certificates was not sufficiently strong, and the private key for the installed certificates was included in software, exposing it. In relation to these issues, alerts were issued after it was revealed that the same problems affected a number of other software programs using the same SDK, as this SDK was actually the root cause*15. Lenovo made these issues public and took measures including the release of a tool for removing this software. After dealing with the problem together with security vendors and other organizations, they reported that the number of affected PCs had decreased*16. However, a U.S. nonprofit organization among others has pointed out that efforts to intercept user communications such as this threaten the privacy and security of users*17.

■ Other

In January, a number of incidents occurred in which malware was distributed via an ad distribution system used on news sites in Canada and the U.S. It has been identified that these attacks exhibited similar properties to attacks redirecting users to malware sites via fake ads on YouTube that occurred in October 2014*18. Attacks using ad distribution systems such as these are also known as malvertising. In Japan, there were incidents in which ad distribution servers used by a number of media outlets and news sites were altered through unauthorized access in 2010*19, and similar incidents have been confirmed since. In addition to alterations, there have also been frequent cases in which users were redirected to malware sites using legitimate ad spots. This is recognized as an efficient method for making large numbers of malware infections possible. We expect that attacks exploiting ad distribution systems like this will continue to occur, so ongoing vigilance is required.

One initiative said to be necessary to improve cyber attack response capabilities is information sharing between the government and citizens, as well as between private companies. However, it has been pointed out that sharing information on threats such as attacks between different organizations or companies is difficult when the handling of said information, including what kind of information is required and which should be shared, is not clearly defined. The U.S. nonprofit organization MITRE Corporation (MITRE)*20 is leading moves to develop the STIX (Structured Threat Information eXpression) description specification using XML. The objective of this specification is to structuralize information on threats such as cyber attacks, aiding their analysis, identification of characteristic events, response management, and information sharing. IPA has published an "Outline of the STIX Format for Structuring and Describing Threat Information," which provides an explanation of this specification*21.

*15 US-CERT, "Vulnerability Note VU#529496 - Komodia Redirector with SSL Digestor fails to properly validate SSL and installs non-unique root CA certificates and private keys" (http://www.kb.cert.org/vuls/id/529496).

*16 Microsoft Malware Protection Center, "MSRT March: Superfish cleanup" (http://blogs.technet.com/b/mmpc/archive/2015/03/10/msrt-march-superfish-cleanup.aspx).

*17 Electronic Frontier Foundation (EFF), "Dear Software Vendors: Please Stop Trying to Intercept Your Customers' Encrypted Traffic" (https://www.eff.org/deeplinks/2015/02/dear-software-vendors-please-stop-trying-intercept-your-customers-encrypted).

*18 Trends Micro Security Intelligence Blog, "YouTube Ads Lead To Exploit Kits, Hit US Victims" (http://blog.trendmicro.com/trendlabs-security-intelligence/youtube-ads-lead-to-exploit-kits-hit-us-victims/).

*19 MicroAd, Inc., "Problem Report: Apology and report regarding alterations on our services" (http://www.microad.co.jp/news/information/detail.php?newid=News-0118) (in Japanese).

*20 MITRE Corporation (http://www.mitre.org/).

*21 IPA, "Outline of the STIX Format for Structuring and Describing Threat Information" (http://www.ipa.go.jp/security/vuln/STIX.html) (in Japanese).

March Incidents

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

S 3rd: An incident occurred in which the website of an airport company was compromised by an unknown party, and altered to redirect visitors to another website.
Narita International Airport Corporation, "Apology for Shutdown of Narita Airport Website & Explanation" (http://www.narita-airport.jp/en/news/150305.html).

V 4th: A vulnerability in TLS/SSL protocols that could allow MITM attacks under certain circumstances was discovered and fixed. This vulnerability was caused by weak RSA encryption from the period when the U.S. restricted encryption exports.
See the following explanation by the discoverer for more information about the attack method. "FREAK: Factoring RSA Export Keys" (https://www.smacktls.com/#freak).

S 7th: It was discovered that the µTorrent BitTorrent client software was installing Bitcoin mining software without users' permission.
See the following µTorrent user forum post for information on the circumstances surrounding this problem. "Warning: EpicScale "riskware" installed with latest uTorrent" (http://forum.utorrent.com/topic/95041-warning-epicscale-riskware-installed-with-latest-utorrent/).

V 10th: It was announced it was possible to elevate privileges using DRAM errors caused by interference between memory cells when they are accessed due to the high density of cells (the rowhammer problem).
See the following Google Project Zero announcement for more details. "Exploiting the DRAM rowhammer bug to gain kernel privileges" (http://googleprojectzero.blogspot.in/2015/03/exploiting-dram-rowhammer-bug-to-gain.html)

O 10th: Following cabinet approval of a bill to amend the Act on the Protection of Personal Information and Number Use Act, the government submitted this bill to the Diet.
Cabinet Secretariat, Bill for Submission to the Diet at the 189th Regular Diet Session "Legislative Bill to Amend Part of the Act on the Protection of Personal Information and Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure" (http://www.cas.go.jp/jp/houan/189.html) (in Japanese).

V 11th: Microsoft published their Security Bulletin Summary for March 2015, and released 14 updates, including five critical updates such as MS15-018, as well as nine important updates.
"Microsoft Security Bulletin Summary for March 2015" (https://technet.microsoft.com/library/security/ms15-mar).

S 11th: A number of websites in Japan were defaced in incidents thought to have exploited a WordPress vulnerability.
National Police Agency, "Regarding the defacement of websites by parties claiming affiliation with 'Islamic State (ISIS)'" (http://www.npa.go.jp/keibi/biki/201503kaizan.pdf) (in Japanese).

O 12th: The National Police Agency made an announcement regarding the state of cyberspace threats in 2014. While there was a drop in the number of arrests for cybercrimes, prefectural police received more inquiries at their consultation counters than the previous year, reaching a record-high number. The techniques used also became more devious and sophisticated, and it is stated that the number and total damages of illegal remittance crimes related to Internet banking were the worst they have ever been.
"Report on Cyberspace Threats for 2014" (http://www.npa.go.jp/kanbou/cybersecurity/H26_jousei.pdf) (in Japanese).

O 12th: IPA published a revised 7th edition of "Building Secure Websites," which summarizes points for developers and operators to take into consideration to prevent unintended damages such as information leaks or alterations affecting websites.
The revised content included the addition of measures regarding a number of attacks such as password list attacks. "How to Secure Your Website" (https://www.ipa.go.jp/security/vuln/websecurity.html) (in Japanese).

V 13th: A number of vulnerabilities in Adobe Flash Player that could allow arbitrary code execution were discovered and fixed.
"APSB15-05: Security updates available for Adobe Flash Player" (https://helpx.adobe.com/security/products/flash-player/apsb15-05.html).

O 17th: The National Diet Library issued their "Problems with Information and Communications" and "Information and Communications Technology Promotion and Cyber Security" research reports. These summarize the current state and issues of policy regarding information and communications, as well as the growing problem of cyber security.
"2015-3-17 Research reports 'Aspects of Information and Communication' and 'Advances in Information and Communication Technology and Cyber Security' (Japanese) published." (http://www.ndl.go.jp/en/news/fy2014/1209642_2113.html).

S 18th: GreatFire.org, which provides information on the status of blocked sites in China, announced it was being targeted by a large-scale DDoS attack.
See the following GreatFire.org blog post for more information about this attack, "We are under attack" (https://en.greatfire.org/blog/2015/mar/we-are-under-attack).

V 26th: Cisco released a scheduled semiannual update for IOS, incorporating a total of seven fixes to issues that could lead to DoS attacks or cause memory leaks.
"Cisco Event Response: March 2015 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication" (http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar15.html).

S 26th: U.S. company GitHub was targeted in a large-scale DDoS attack that spanned several days.
See the following GitHub announcement for more information, "Large Scale DDoS Attack on github.com" (https://github.com/blog/1981-large-scale-ddos-attack-on-github-com).

O 31st: IPA published "Effective Vulnerability Countermeasure Procedures (Practical Edition)," which summarizes advice regarding the collection of vulnerability information and utilization of such information to deal with vulnerabilities effectively.
"IPA Technical Watch 'Effective Vulnerability Countermeasure Procedures (Practical Edition)'" (http://www.ipa.go.jp/security/technicalwatch/20150331.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 March, U.S. company GitHub was targeted in a large-scale DDoS attack that spanned several days *22. It has been identified that JavaScript on a Chinese search service provider may have been altered by an unknown party when accessed from outside China so that it could be used in these attacks*23.

Also in March, there was an incident in which certificates for a number of Google domains were issued without authorization by an intermediate certificate authority in Egypt. These certificates were each revoked on major browsers. In this incident, it is said the only confirmation of the validity of an application for a certificate was a check to see whether an email address at the domain name the certificate was for could be contacted. Additionally, after learning that the confirmation of application validity upon issue was lacking at a number of certificate authorities in this way, an alert was issued*24.

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 January 1 and March 31, 2015.

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*25, attacks on servers*26, and compound attacks (several types of attacks on a single target conducted at the same time).

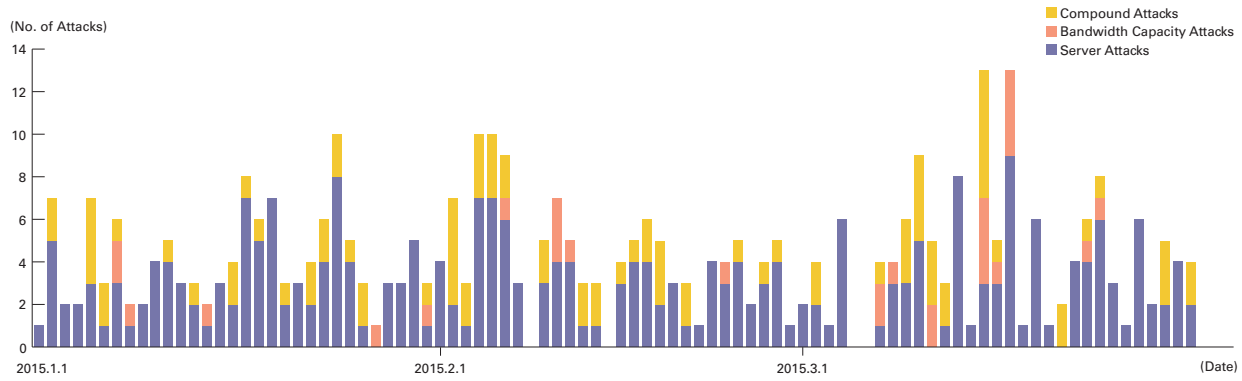


Figure 2: Trends in DDoS Attacks

*22 See the Sophos Naked Security blog post, "Greatfire.org faces daily $30,000 bill from DDoS attack" (https://nakedsecurity.sophos.com/2015/03/20/greatfire-org-faces-daily-30000-bill-from-ddos-attack/) for more information about this attack.

*23 See the following report for more information on this attack method. "Using Baidu 百度 to steer millions of computers to launch denial of service attacks" (https://drive.google.com/file/d/0ByrxbIDXR_yqeUNZYU5WcjFCbXM/view).

*24 US-CERT, "Vulnerability Note VU#591120 - Multiple SSL certificate authorities use predefined email addresses as proof of domain ownership" (http://www.kb.cert.org/vuls/id/591120)

*25 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.

*26 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.

During the three months under study, IIJ dealt with 384 DDoS attacks. This averages to 4.27 attacks per day, indicating an increase in the average daily number of attacks compared to our prior report. Server attacks accounted for 69.3% of all incidents, while compound attacks accounted for 23.4%, and bandwidth capacity attacks 7.3%. The largest attack observed during the period under study was classified as a compound attack, and resulted in 2.83 Gbps of bandwidth using up to 1,179,000 pps packets.

Of all attacks, 82.6% ended within 30 minutes of commencement, 17.4% lasted between 30 minutes and 24 hours, and none lasted over 24 hours. The longest sustained attack was a compound attack that lasted for ten hours and 37 minutes.

In most cases, we observed an extremely large number of IP addresses, whether domestic or foreign. We believe this is accounted for by the use of IP spoofing*27 and botnet*28 usage as the method for conducting DDoS attacks.

■ Backscatter Observations

Next we present our observations of DDoS attack backscatter using the honeypots*29 set up by the MITF, a malware activity observation project operated by IIJ*30. By monitoring backscatter it is possible to detect some of the DDoS attacks occurring on external networks as a third party without any interposition.

For the backscatter observed between January 1 and March 31, 2015, Figure 3 shows the sender's IP addresses classified by country, and Figure 4 shows trends in packet numbers by port.

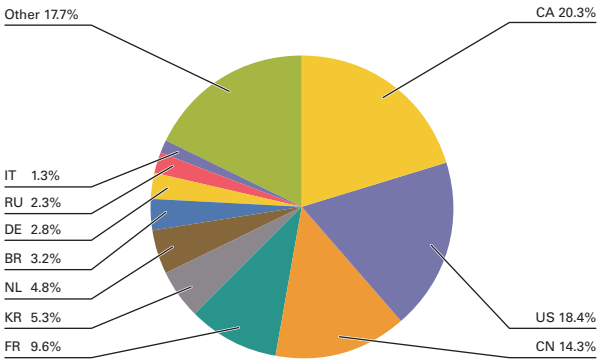


Figure 3: DDoS Attack Targets by Country According to Backscatter Observations

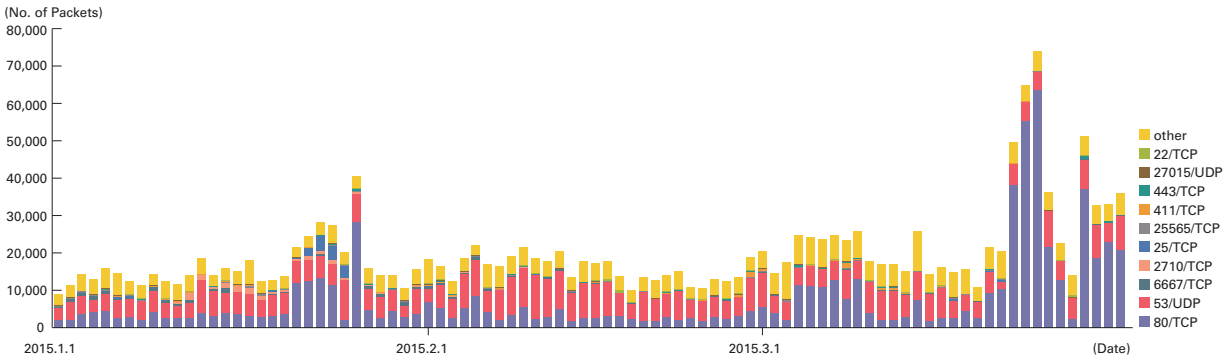


Figure 4: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)

*27 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.

*28 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.

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

*30 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."

The port most commonly targeted by the DDoS attacks observed was the 80/TCP port used for Web services, accounting for 38.2% of the total during the target period. This was followed by 53/UDP used for DNS at 31.8%, so the top two ports accounted for 70% of the total. Attacks were also observed on 6667/TCP used for IRC (Internet Relay Chat), 25/TCP used for SMTP, and 443/TCP used for HTTPS, as well as the typically unused 2710/TCP, 25565/TCP, and 27015/UDP.

Examining the daily average number of packets for the 53/UDP communications observed often since February 2014, we can see there is still an upward trend, with it rising to around 6,200 from around 3,900 in the previous survey period.

Looking at the origin of backscatter thought to indicate IP addresses targeted by DDoS by country in Figure 3, Canada accounted for the largest ratio at 20.3%. The United States and China followed at 18.4% and 14.3%, respectively.

Regarding particularly large numbers of backscatter packets observed, there were attacks on the Web servers (80/TCP) for a hosting provider in Canada on between January 21 and January 26. From March 20 continued attacks on this provider were observed, focusing on a number of websites related to a game made in China. Additionally, attacks were observed on a U.S. hosting provider between March 4 and March 9. Regarding attacks on other ports, between January 22 and January 25 there were attacks on 25/TCP targeting a game-related site in France.

Notable DDoS attacks during the current survey period that were detected via IIJ's observations of backscatter included attacks on a Finnish financial institution group between January 1 and January 4, and attacks on Islamic extremist sites carried out by Anonymous on January 11 (OpCharlieHebdo). Attacks on GitHub were also detected between March 27 and March 29. Regarding these attacks on GitHub, because the reported attack method does not generate backscatter, we know that another method was also used at the same time.

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the MITF*31, a malware activity observation project operated by IIJ. The MITF uses honeypots*32 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.

*31 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.

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

■ Status of Random Communications

Figure 5 shows the distribution of sender's IP addresses by country for communications coming into the honeypots between January 1 and March 31, 2015. Figure 6 shows trends in the total volumes (incoming packets). The MITF has set up numerous honeypots for the purpose of observation. We have taken the average per honeypot, showing the trends for incoming packet types (top ten) over the entire period subject to study. Additionally, in these observations we corrected data to count multiple TCP connections as a single attack when the attack involved multiple connections to a specific port, such as attacks on MSRPC.

Much of the communications arriving at the honeypots demonstrated scanning behavior targeting TCP ports utilized by Microsoft operating systems. We also observed scanning behavior targeting 1433/TCP used by Microsoft's SQL Server, 22/TCP used for SSH, 23/TCP used for Telnet, 8080/TCP used for HTTP-proxy, ICMP echo requests, 80/TCP and 443/TCP used for HTTP, and 3389/TCP used for RDP. The increase in communications targeting Telnet (23/TCP) since November in the previous survey period continued until February. Upon investigation, we learned that this was mainly received from IP addresses allocated to China and Japan. Between February 17 and February 20, there was a spike in communications from many IP addresses allocated to countries such as China, the United States, Hong Kong, Taiwan, and Russia. Most of these communications were scanning behavior attempting to find SSH, Telnet, or proxy servers. Between March 21 and March 23, there was an increase in communications from a large number of IP addresses allocated to countries including China and the United States, and this followed a similar trend.

■ Malware Network Activity

Figure 7 shows the distribution of the specimen acquisition source for malware during the period under study, while Figure 8 shows trends in the total number of malware specimens acquired. Figure 9 shows trends in the number of unique specimens. In Figure 8 and Figure 9, the number of acquired specimens show the total number of specimens acquired per day*33, while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*34. 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 reports, for Figure 8 and Figure 9 we have detected Conficker using multiple anti-virus software packages, and removed any Conficker results when totaling data.

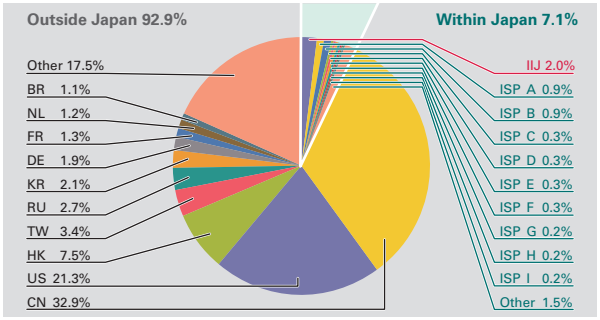


Figure 5: Sender Distribution (by Country, Entire Period under Study)

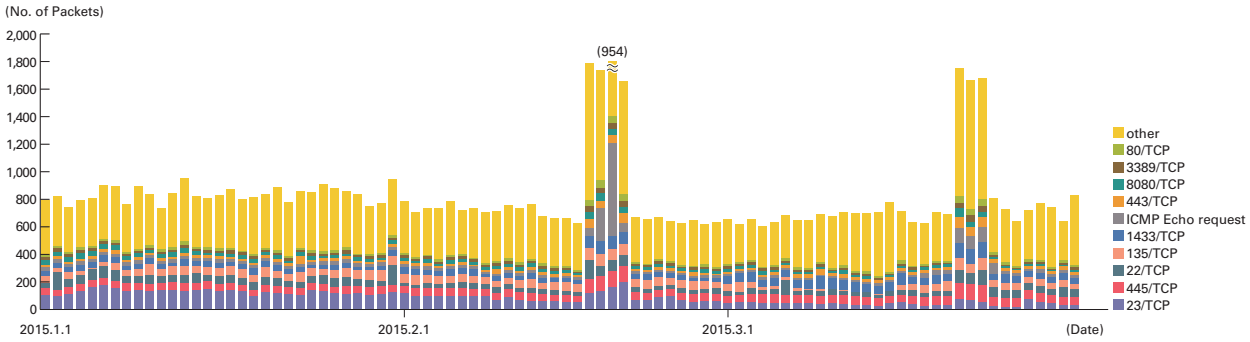


Figure 6: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

*33 This indicates the malware acquired by honeypots.

*34 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.

On average, 87 specimens were acquired per day during the period under study, representing 19 different malware. After investigating the undetected specimens more closely, they included worms observed from IP addresses allocated to countries such as China, the United States, India and Taiwan. Additionally, about 49% of undetected specimens were in text format. 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 websites that newly-infected PCs access to download malware.

Under the MITF's independent analysis, during the current period under observation 94.3% of malware specimens acquired were worms, 2.3% were bots, and 3.4% were downloaders. In addition, the MITF confirmed the presence of 105 botnet C&C servers*35 and 14 malware distribution sites. The number of botnet C&C servers continues to rise sharply as seen in the previous survey period, but this was due to the appearance of a specimen that used a DGA (Domain Generation Algorithm) during the current survey period.

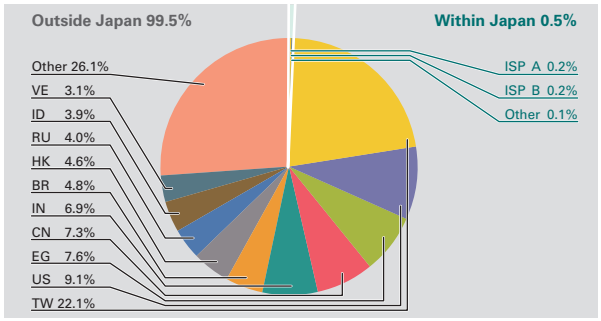


Figure 7: Distribution of Acquired Specimens by Source (by Country, Entire Period under Study, Excluding Conficker)

Conficker Activity

Including Conficker, an average of 19,434 specimens were acquired per day during the period covered by this report, representing 608 different malware. While figures rise and fall over short periods, Conficker accounts for 99.5% of the total number of specimens acquired, and 97.0% of unique specimens. This demonstrates that Conficker remains the most prevalent malware by far, so we have omitted it from figures in this report. Compared to the previous survey period, the total number of specimens acquired increased by approximately 19% during the period covered by this report, and the number of unique specimens increased by

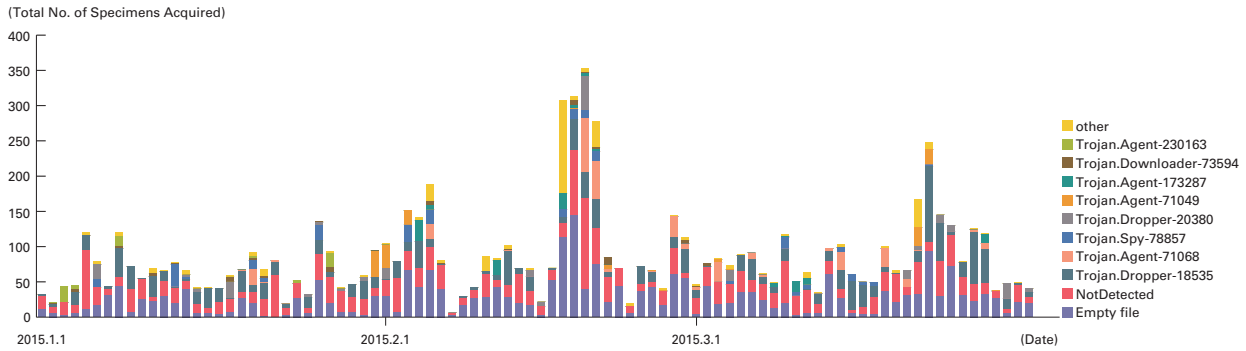


Figure 8: Trends in the Total Number of Malware Specimens Acquired (Excluding Conficker)

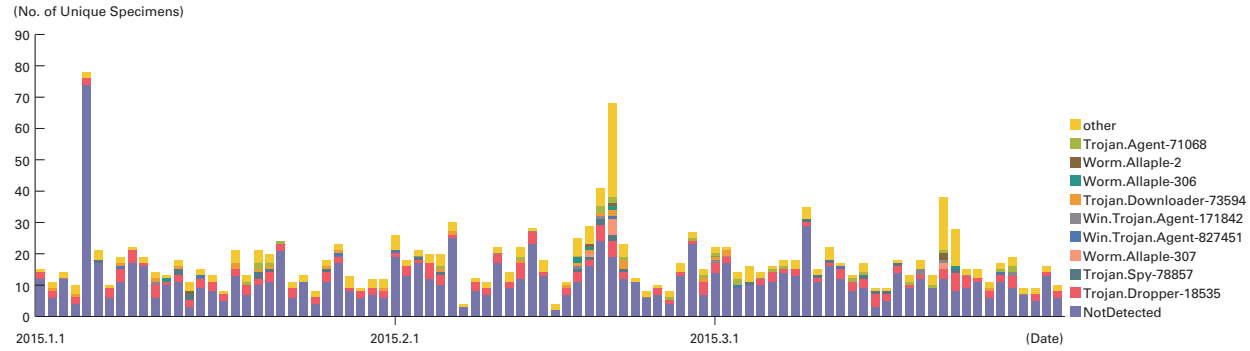


Figure 9: Trends in the Number of Unique Specimens (Excluding Conficker)

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

about 9%. According to the observations of the Conficker Working Group*36, as of April 3, 2015, a total of 707,844 unique IP addresses are infected*37. This indicates a drop to about 22% of the 3.2 million PCs observed in November 2011, but it demonstrates that infections are still widespread.

1.3.3 SQL Injection Attacks

Of the types of different Web server attacks, IIJ conducts ongoing surveys related to SQL injection attacks*38. SQL injection attacks have flared up in frequency numerous times in the past, and remain a major topic in 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 January 1 and March 31, 2015. Figure 11 shows trends in the numbers of attacks. These are a summary of attacks detected by signatures on the IIJ Managed IPS Service.

China was the source for 90.8% of attacks observed, while the United States and Japan accounted for 2.5% and 2.3%, respectively, with other countries following in order. There was a dramatic increase in the number of SQL injection attacks against Web servers compared to the previous report. This was mainly due to a significant spike in attacks from China, with several large-scale attacks occurring.

During this period, attacks from multiple attack sources in China directed at specific targets took place on February 13. On February 16, attacks were also made from a number of other sources directed at multiple targets. Between February 20 and February 23, there were large-scale attacks from a number of sources in China against multiple targets. One of these attack targets was also attacked from another source in China between March 27 and March 30. Attacks on this target accounted for 66.3% of the overall attacks that occurred during this survey period. Attacks were made from multiple sources, with over 400,000 attacks observed from a single attack source in more than one case. Because most of the companies targeted by attacks were connected to finance, it is believed that these were large-scale attempts to find vulnerabilities on Web servers of the financial industry.

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.

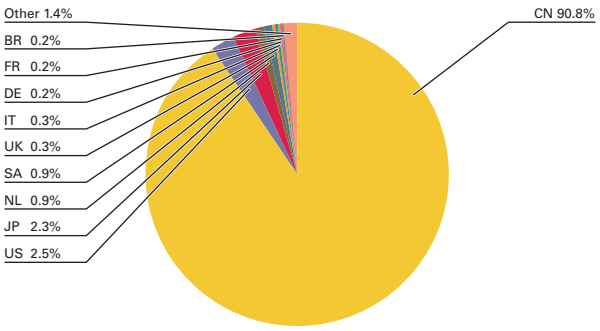


Figure 10: Distribution of SQL Injection Attacks by Source

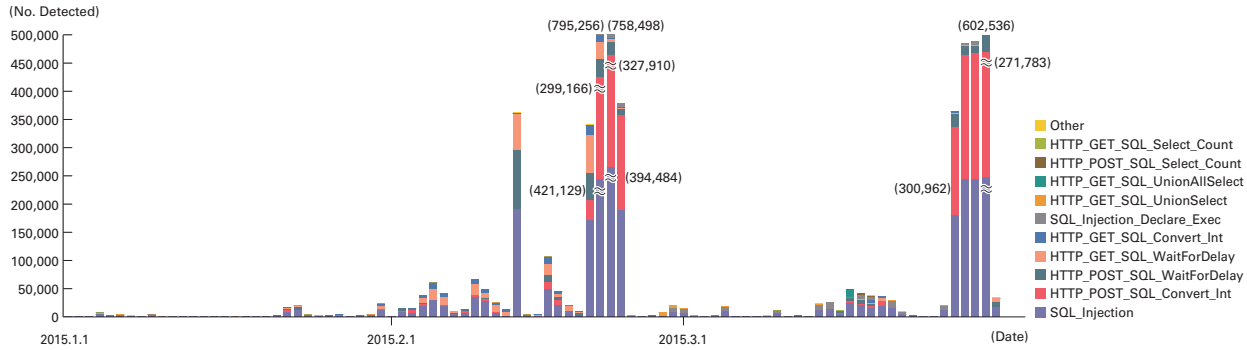


Figure 11: Trends in SQL Injection Attacks (by Day, by Attack Type)

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

*37 For some reason Conficker Working Group data appears to be missing between March 28 and April 2, 2015, so we have cited data for April 3, 2015 that should not be affected.

*38 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.

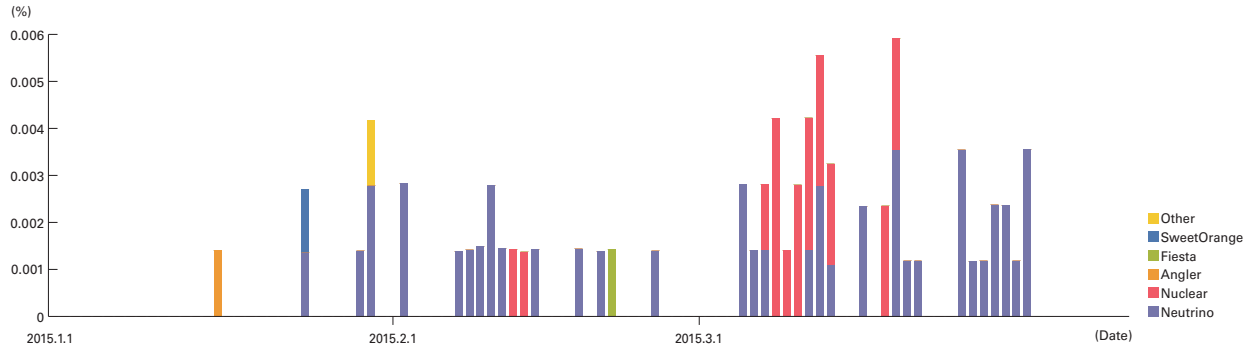
1.3.4 Website Alterations

Here we indicate the status of website alterations as surveyed through the MITF Web crawler (client honeypot)*39.

This Web crawler accesses tens of thousands of websites on a daily basis, with a focus on well-known and popular sites in Japan. We also add new target sites on a regular basis. In addition to this, we temporarily monitor websites that have seen short-term increases in access numbers. By surveying websites thought to be viewed frequently by typical users in Japan, it is easier to speculate on trends regarding fluctuations in the number of altered sites, as well as the vulnerabilities exploited and malware distributed.

The number of drive-by download attacks observed between January and March 2015 continued the declining trend seen in the October to December 2014 period, and fell by around another 10 percent (Figure 12). In January in particular, almost no activity was observed. Additionally, following an increase in attack numbers from the latter half of February, there tended to be sharp drops in the number of attacks detected during weekends. As for the composition of attacks, the majority consisted of either Nuclear, which we have been detecting since we began operating this Web crawler, or Neutrino, which had not detected since February 2014*40. Each of these exploit kits, like many of the other exploit kits that are popular recently, is equipped with functions for exploiting Flash vulnerabilities (such as CVE-2014-0515, CVE-2014-0569, CVE-2015-0313, and CVE-2015-0336), and functions for exploiting new vulnerabilities are added at a fast pace*41. In most cases, the websites altered to redirect visitors were observed intermittently acting as a redirection source over an extended period (more than three months). Regarding trends in content, the sites observed included those that introduce adult video content, as well as websites for small and medium-scale content providers. These trends remain unchanged.

Overall, although the incidence rate for drive-by downloads was very low, it can be said that it is now in a slight uptrend. Because Nuclear and Neutrino that were commonly observed in this survey period have been linked to Operation Windigo*42*43, attacker groups may wield a comparatively large amount of potential power. It is recommended that all parties continue to exercise caution. Website operators should ensure that measures against the alteration of web content are in place, and visitors should stay up to date with measures against vulnerabilities in browsers or related plug-ins (Flash Player in particular).



*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 12: Rate of Drive-By Download Incidence When Viewing Websites (%) (by Exploit Kit)

*39 See "1.4.3 Website Defacement Surveys Using Web Crawlers" in Vol.22 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol22_EN.pdf) for an explanation of Web crawler observation methods.

*40 The Neutrino Exploit Kit spread like wildfire in Japan and internationally from around October 2013, but gradually died down, and this Web crawler had not detected it since February 2014. That said, in November 2014 the release of a new version was reported in an article titled, "Neutrino : The come back! (or Job314 the Alter EK)" (http://malware.dontneedcoffee.com/2014/11/neutrino-come-back.html).

*41 For example, in "CVE-2015-0336 (Flash up to 16.0.0.305) and Exploit Kits" (http://malware.dontneedcoffee.com/2015/03/cve-2015-0336-flash-up-to-1600305-and.html), it is reported that a vulnerability disclosed on March 12, 2015, was confirmed to be exploited by Nuclear on March 19, and by Neutrino on April 2.

*42 Large-scale attack activity disclosed in the ESET white paper, "OPERATION WINDIGO" (http://www.welivesecurity.com/wp-content/uploads/2014/03/operation_windigo.pdf). It is reported that since 2011, more than 25,000 servers have been compromised and exploited to send spam or redirect clients.

*43 Regarding connections to Operation Windigo, see "HAPPY NUCL(Y)EAR - EVOLUTION OF AN EXPLOIT KIT" (http://community.websense.com/blogs/securitylabs/archive/2015/01/15/evolution-of-an-exploit-kit-nuclear-pack.aspx) for more information on Nuclear, and "Exploit Kit Evolution - Neutrino" (https://isc.sans.edu/diary/Exploit+Kit+Evolution+-+Neutrino/19283) for more information on Neutrino.

1.4 Focused Research

Incidents occurring over the Internet change in type and scope from one minute to the next. Accordingly, IIJ works toward implementing countermeasures by continuing to perform independent surveys and analyses of prevalent incidents. Here we will present information from the surveys we have undertaken during this period regarding increasingly malicious PUAs, ID management technology, and evaluation of the IOCs of malware that reprograms HDD firmware.

1.4.1 Increasingly Malicious PUAs

PUA is an abbreviation of Potentially Unwanted Application, and refers to software that is either not needed by users in the first place, or that includes some inappropriate functions despite being beneficial overall. They are also known as PUPs (Potentially Unwanted Programs). Adware that forcibly inserts advertising while the software is being used is sometimes treated as a type of PUA as well. Although some PUAs appear to be harmless and simply provide legitimate functions at first glance, there are also malicious PUAs that acquire information on user behavior and send it to external sources for use in advertising, etc., without the user being aware. Additionally, in recent years there has been an increasing number of malicious PUAs that use techniques similar to malware, tricking users into installing PUAs, using them to steal information, and also installing other PUAs, altering Web content, and elevating privileges by bypassing UAC. In this report, we examine the results of IIJ's recent analysis of a number of PUAs, and discuss the techniques they used.

■ Defining PUAs

The strict definition of a PUA differs even among experts. That is because going by the literal definition, all programs with functions that are unwanted by users can be considered PUAs, regardless of whether or not they are malicious. Whether a program is unwanted by a user varies based on factors such as their attitude, point of view, situation, and environment. Consequently, here we will define PUAs as all unwanted programs installed in addition to software a user intended to install, despite having no relation to it. We will refer to examples among these that use techniques similar to malware as malicious PUAs.

■ Examples of Malicious PUAs

Intrusion Route

Attackers often manipulate Web search engine results in advance through techniques such as SEO poisoning*44 to redirect users to fraudulent sites. For example, when searching for a certain piece of software you want to download by entering the software's name and version along with keywords such as "download," there have been cases in which a fraudulent site is displayed with a higher ranking than the original distribution site. In other cases, fraudulent distribution sites are mixed in with the ads displayed together with the search results. The fraudulent sites that users are redirected to sometimes feature domain names and designs that resemble famous download sites, making it harder to identify them as fraudulent. There have also been fake download buttons that induce users to download malicious PUAs amongst the ads on the Web pages of a number of well-known download sites. Figure 13 shows a sample design for a download site. There are multiple ad-based fraudulent download buttons mixed in with others, so users unfamiliar with the website will be unlikely to know which is the real download button. Furthermore, several well-known download sites use their

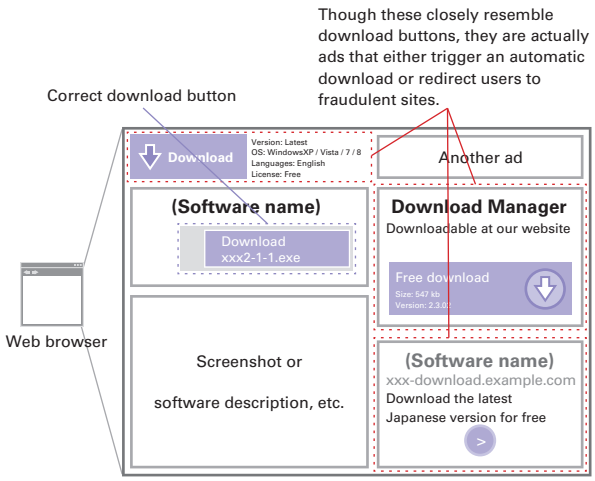


Figure 13: Examples of Fake Download Buttons (Ads) Inserted into Download Sites

*44 SEO (Search Engine Optimization) poisoning is a technique for displaying a page you have prepared higher than it normally would be ranked by using the search engine optimization algorithm to intentionally manipulate search results. It was originally a marketing technique, but now it is also used to cause harm to users through malware infections, etc.

own dedicated download tool, and have users download the software they want to install through this tool. However, in some cases PUAs are bundled in with these tools. There are also cases in which download sites offer installers bundled with PUAs after obtaining permission from individual software creators.

PUA Implementation Framework

Some PUAs that users are induced to download are individual pieces of adware, but in other cases they have been downloader programs that go on to install multiple PUAs. In one example, a diverse range of additional PUAs were downloaded, with the number and type varying from one minute to the next. This is thought to indicate that the person who built the PUA framework was running a pay-per-install*45 operation, installing PUAs on user systems based on client requests for financial gain.

Downloader-type PUAs communicate with a C&C server periodically after they are installed, updating themselves and downloading new PUAs. Additionally, in many cases PUAs also install the software users originally intended to install, making it harder for users to realize they have been deceived.

For installer-type PUAs, there are also cases in which designs that users find confusing are intentionally used to get users to unwittingly consent to install a PUA during the installation process. Figure 14 is an example of an adware installer design. It is made to appear as the installer for the software the user wants to install, but the terms of license text refers to other adware, and this adware is installed in the background when the user clicks "CONTINUE". Unless the user is paying close attention during installation, they are deemed to have consented to installing the adware.

Some PUAs were installed without obtaining user consent. If PUAs like this are executed, even if the user rejected installation of the software shown, it will remain on the PC, and continue to download new PUAs and attempt to update itself. Some additionally downloaded PUAs were also installed without obtaining user consent.

Web Content Alteration

Some PUAs were run as Web browser plug-ins or extensions, or the code for the PUA itself was injected into a Web browser to hook the send and receive APIs, and hijack them to steal all the URLs a user had accessed. Ads based on these were then inserted into the Web content being viewed to alter it. Although the content inserted differs, this is similar to banking Trojans such as ZeuS, SpyEye, and Vawtrak*46 that use the WebInject technique*47. Software that uses this type of attack method is also known as a Web browser hijacker.

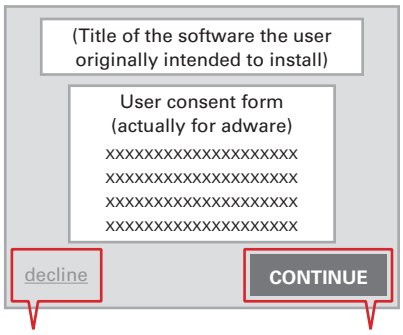


Figure 14: Example of PUA Installer Design

*45 Pay-per-click reward affiliates are also called pay-per-access, with rewards determined based on the number of ads that are clicked. Similarly, pay-per-install rewards are determined based on the number of software installations made. For example, if the client is a creator of adware that earns money by making users access affiliate sites repeatedly, having this adware installed on as many PCs as possible boosts their potential earnings. That is why they send requests to organizations with this kind of framework. The consignee is believed to build frameworks like this because they receive a greater financial reward from the client for inducing more installations. It is said this model has also been used with malware in recent years.

*46 See "1.4.3 ZeuS and its Variants" in Vol.16 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol16_EN.pdf) for more information on ZeuS. See "1.4.2 SpyEye" in Vol.13 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol13_EN.pdf) for more information on SpyEye. See "1.4.2 The Vawtrak Malware That Steals Authentication Information, etc. for Japanese Financial Institutions" in Vol.24 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol24_EN.pdf) for more information on Vawtrak. The Citadel variant of ZeuS with WebInject functions is also detailed in "1.4.2 The Citadel Variant of ZeuS" in Vol.18 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol18_EN.pdf).

*47 WebInject is a function for altering Web content in browser memory by setting hooks for the Web browser's communication system API. Most banking Trojan malware such as ZeuS and SpyEye have functions like this to deceive a user into entering additional information such as a passcode for two-factor authentication when the user logs in to a financial institution. The stolen authentication information is used to attempt to misappropriate funds. A detailed explanation of WebInject can be found in IIR Vol.18 (http://www.iij.ad.jp/en/company/development/iir/018.html) under "1.4.2 The Citadel Variant of ZeuS," or IIR Vol.13 (http://www.iij.ad.jp/en/company/development/iir/013.html) under "1.4.2 SpyEye."

Other techniques include installing a self-signed root certificate, and having the PUA itself act as a local proxy for HTTP(S), causing all communications from the Web browser to be sent to it. Certificates from Web servers are then intercepted, altered, and signed using the root certificate that the PUA installed itself. Some variants discovered use this technique to intercept communications via a MITM*48 attack, and alter content by inserting ads, etc.

Both techniques enable alterations to even encrypted HTTP communications content without users noticing, so they are extremely dangerous. There are also examples that operate as a Web browser toolbar, forcing the use of a search engine provided by an adware supplier, and intercepting search keywords.

Exploiting Windows Specifications

Malware such as PlugX*49 and Dridex*50 each use different techniques to bypass UAC*51 pop-ups, and are equipped with functions to automatically gain administrator privileges. A number of the PUAs we analyzed in this survey also incorporated functions for elevating privileges in this way (most using the same method as Dridex). This is because it is necessary for a PUA to gain administrator privileges to subsequently install multiple additional PUAs to the system folder without the user noticing.

Obfuscation

A number of PUAs downloaded additional PUAs that were compressed using a custom format or obfuscated, and these were difficult to detect using IDS or IPS because they were not in executable format while traveling over the communications route. Furthermore, the PUAs themselves also implemented code obfuscation or the obfuscation of key character strings, making it harder to detect and analyze their characteristics.

Anti-Sandbox Techniques

A number of PUAs were only added to the startup programs when installed, so they were not executed until the next time the PC was rebooted. This behavior is designed to evade detection by sandbox products that use dynamic analysis for rapid detection, and this same technique is used by some malware. Even when attempting to execute them manually or reboot the PC directly after installation, although communications with the C&C server took place, they were configured to not download new PUAs from the server immediately. Instead, new PUAs were downloaded after anywhere from a few days to several months had passed. This is also thought to be a technique for evading detection by sandboxes.

*48 A MITM (Man-In-The-Middle) attack is a technique in which the attacker interposes themselves between two communicating parties to steal communications, decrypting them to intercept or alter the content without users noticing.

*49 See "1.4.1 The PlugX RAT Used in Targeted Attacks" in Vol.21 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol21_EN.pdf) and the "I Know You Want Me - Unplugging PlugX" Black Hat Asia 2014 presentation (https://www.blackhat.com/docs/asia-14/materials/Haruyama/Asia-14-Haruyama-I-Know-You-Want-Me-Unplugging-PlugX.pdf) for more information about PlugX. The elevation of privileges by bypassing UAC is also discussed within.

*50 See the JPCERT/CC Analysis Center article, "The New UAC Bypass Method Used by Dridex" (https://www.jpcert.or.jp/magazine/acreport-uac-bypass.html) (in Japanese) for more information on the UAC bypass technique used by Dridex.

*51 Windows versions from Windows Vista onward include a function called UAC (User Account Control) that disables key privileges under normal circumstances even when an account with administrator privileges is logged in. A pop-up prompting the user for permission is displayed when a program performs a critical operation that changes the system, and privileges are only given if permission is granted. There are four levels of UAC control, but from Windows 7 onward Microsoft made the second highest of the four levels the default due to user requests (in Vista the highest level was the default). At this level, a UAC popup is not displayed when Windows determines that an action was performed by a user, and privileges are elevated automatically. In recent years, malware has exploited this specification in a number of attack methods that make actions appear as if they were performed by a user, so administrator privileges are granted automatically without displaying a UAC pop-up.

VM Detection

Many malware specimens have functions for interfering with execution in a virtual environment or sandbox, and similar functions were also found in the PUAs we analyzed here. In particular, virtual environments such as Hyper-V, Xen, and KVM that I have not seen when analyzing malware in the past were also detected. Detection was carried out using the WMI and WBEM*52 functions to obtain BIOS information. In combination with other techniques, it is possible to detect almost all virtual environments, and systems that change the behavior of the PUAs to prevent execution upon detection were incorporated. This is another way that they interfere with analysis.

The Risk of PUA Infections at Organizations

The Web browser hijacker PUAs discussed here send all information such as the URLs of websites visited by users to an external party. If an organization is infected with this kind of PUA, details such as Intranet server names, URL path information, and GET parameters will also be leaked. This is undesirable from the perspective of protecting the internal information of organizations such as companies.

Furthermore, there is a risk of malware being included among the additional programs installed by PUA frameworks. In recent years there have also been cases in which ad sites themselves have been altered*53, leading to malware being installed via drive-by downloads*54. The risk of infection through users being redirected to a malicious website when viewing an ad displayed by adware cannot be excluded. To avoid this situation, it is a good idea to carry out monitoring to prevent PUAs or any software unwanted by the organization or user from being installed. You should also construct a system that enables you to deal with infections swiftly if they are discovered.

Countermeasures

To avoid being infected by malicious PUAs, users themselves must first become familiar with the official sites of the software that they use. By always using only the official site, or legitimate mirror sites reached from there, it is possible to prevent the download of malicious PUAs from fraudulent websites. There is also the risk of downloading PUAs by clicking malicious ads posing as download buttons, so techniques such as checking the hash values listed on the official site are one other way of preventing people falling for this trick*55. Furthermore, it is always best to avoid installing software that has a dubious reputation or is from an unreliable source without taking the proper precautions. If you are an administrator, it is a good idea to consider granting users only general user privileges to prevent them installing software arbitrarily. In addition, because some software can be installed in user directories, you can stop users from downloading and using software freely by prohibiting the execution of programs outside the system directory and program files folder, via Windows functions such as software restriction policies or AppLocker.

Some well-known or pre-installed software may also attempt to install PUAs when they are installed or updated. Take care not to click the “Next” button too quickly without reading the details.

*52 WBEM (Web-Based Enterprise Management) is a technical specification for managing distributed computing. It was drawn up by the DMTF (Desktop Management Task Force) industry standards group. WMI is short for Windows Management Instrumentation, which is an implementation for managing Windows using WBEM. WMI can perform tasks such as obtaining a variety of local and remote Windows information (all manner of information such as hardware, software, OS, users, and processes), and changing the status.

*53 The attack technique in which an attacker alters an ad platform to set up an exploit within is called malvertising. Malvertising is a coined term that combines “malicious” and “advertising.” In many cases ad platforms distribute ads to multiple websites, and when they are altered it is possible to distribute an exploit to all of these websites at once. Because this is efficient for attackers, in recent years these platforms have been targeted frequently. There are also cases in which attackers themselves directly distribute ads for redirecting users to malware sites.

*54 Drive-by downloads cause malware infections by exploiting some kind of vulnerability when a user views Web content. If the computer used by the viewer is vulnerable, it is infected with malware merely by viewing the Web content.

*55 The importance of confirmation using hash values is discussed in detail under “1.4.3 Alteration of Software Distribution Packages” in Vol.10 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol10.pdf).

Additionally, because there have been incidents in which adware has been found in software pre-installed on PCs, caution must be exercised when procuring PCs. A number of manufacturers specify a list of pre-installed software, so refer to this when selecting PCs. Furthermore, some manufacturers enable the customization of PCs for business use, so you can have them shipped with the pre-installed software removed. Procuring PCs like this is one method to consider.

Other than that, it will also be necessary to implement similar measures as for malware, due to the possibility of vulnerabilities being exploited to force installation*56. As we have discussed here, there are also malicious PUAs that exploit Windows specifications to bypass UAC. For this reason, those managing PCs with an administrator account should look into raising UAC to the highest level.

1.4.2 ID Management Technology: From a Convenience and Security Perspective

Continuing on from the previous report, here we will once again discuss ID (identity) management. We discussed IDs under the narrow definition of identifiers, and took a look at the relationship between private token and public credential information. We also examined the difference between authentication and authorization, and explained the process from authentication using tokens and circulation of the various credentials to finally granting access privileges. In this report, we will talk about how these technologies are actually used, including some specific examples.

■ ID and Token Variation

In the previous report, we explained the process by which an entity with an ID is authenticated to associate attributes and authorization information with the corresponding ID, and issue credential information associated with them. At the time of authentication, tokens are used to guarantee the reliability of the entity with that ID. Because authentication is carried out for an individual realm (valid areas of the authentication and authorization process), entities in each realm generally have ID and token pairs. In this report, we will present use cases in which ID and tokens are actually used.

In a realm there is an IdP (identity provider) that performs authentication-related tasks, and an entity in the said realm is assigned a unique ID. This can be thought of as the registration screen you input the necessary details into when using an online service for the first time. When registering, there is a “user ID” or similar field for entering an ID, and a check is performed to ensure that the ID is not already in use by another user. On the other hand, there are cases in which a random ID is assigned on the service side. In either case, personal data such as an email address or phone number is normally also entered upon user registration. Registration is only provisional at this stage, so notification is sent along with a “challenge” by way of an email to the email address entered or a short message to the phone number, and the user’s identity is confirmed by having them input the corresponding challenge. During provisional registration or input of the challenge, a password as a type of token is generally chosen. In this way, use of the service is possible once registration of the ID and password pair is complete.

There are now cases in which an email address is substituted rather than assigning an ID unique to a realm. This is done to reduce the cost for managing IDs within a realm, and because it has the added benefit of avoiding situations where an ID selected by the user, or in particular a random ID assigned by the IdP, is forgotten. When assigning IDs unique to a realm, it is necessary to operate a Web page for providing ID reminders or resetting the password by prompting users to enter the email address or phone number used to confirm their identity, and this increases the burden on the service side. Meanwhile, when using an email address as the ID, you must consider the fact that it may be targeted in list-based attacks. It could be said that there is the same risk when identical IDs are reused on each realm. Of course, not reusing the same password is a fundamental countermeasure against this, but the name binding or collation of leaked data due to IDs being identical is also a risk*57. Additionally, there have been cases in the past where the leak of private information has been caused by entering the email address of an acquaintance on a reminder page for the input of IDs on an SNS or shopping site due to email addresses being used as IDs. In light of these circumstances, we are now seeing systems that issue IDs unique to a realm, but also give users the right to choose whether or not to use their email address during the login process.

*56 See Vol.21 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol21_EN.pdf) at the end of “1.4.1 The PlugX RAT Used in Targeted Attacks” for more information about malware infection countermeasures in client environments.

*57 This is of course not limited to ID-based name collation, as the threat of name collation through information such as the name or phone number entered at the time of registration still remains.

This shows that although IDs were thought of as public information in the past, there are also cases where it is recognized that they should be kept confidential. We will now examine the concept of using base IDs and derivative IDs as a way to deal with this issue. When various portal sites or SNS sites are used as IdPs, there are cases in which the site provides a range of services with the same ID and token. In these cases, there are situations in which you want to change your perspective based on the service, and you do not want it to be known that your words or actions are being made by the same entity. This leads to the idea of treating the ID first assigned to you as your base ID, and deriving different IDs from it for each situation in which an ID is actually used. This serves as a simple way to prevent situations where, as mentioned previously, the leak of the IDs is in itself a threat. When logging in using a derivative ID, a token associated with the base ID is used, eliminating the confusion of having to manage individual tokens for each derivative ID. It is also not necessary to re-enter the token when logging in again, making it possible to perform actions using different derivative IDs for each service by simply switching between derivative IDs. One point that should be noted is that there may be cases where you forget which derivative ID you are logged in under, leading to multiple activities by users that appear different from the perspective of a third party being associated. For example, it is necessary to pay attention to information such as the nickname displayed when you log in.

The concept of derivative tokens can be considered similar to the idea of derivative IDs. This technique involves the use of a base ID and derivative token pair for authentication by linking a derivative token to a base ID separately from the base token. When you think of this derivative token as a single-use token, it can also be considered as a type of one-time password. As far as the actual purpose of this goes, one possible use could be saving derivative tokens for each application on a smartphone (this could include cases in which tokens are encrypted using a master password and stored, rather than using the actual token itself). This would be a useful function in environments such as smartphones where password input is difficult. This also has the benefit of limiting the damage caused if a password were to leak from a specific application and be disclosed. Another advantage is that you only have to disable the derivative password, so the base password does not need to be changed. From this perspective, you can think of it as delegation and can limit the scope of the authorization when a derivative token is used in comparison to the scope of the authorization for the base token. This enables you to minimize the impact if the token leaks.

As this demonstrates, it is best to consider the balance between user convenience (forgetting IDs) and security (the reuse of IDs or leak of tokens). Furthermore, by expanding upon the concept of derivative IDs and tokens, authentication and authorization systems that use neither base IDs nor base tokens are also possible, as shown in Figure 15. There are no systems actually using a method like this right now, but a new approach like this may be implemented at some point based on the future needs of users who place emphasis on protecting their privacy.

■ One-Time Password Variation

Above we discussed variations regarding the use of IDs and tokens. Next we will examine one-time passwords, which are a type of token that is used once and then discarded. One-time passwords have mainly been used in Internet banking systems up to this point, and they were seen as a secure authentication method. However, in February 2015, Japan's National Police

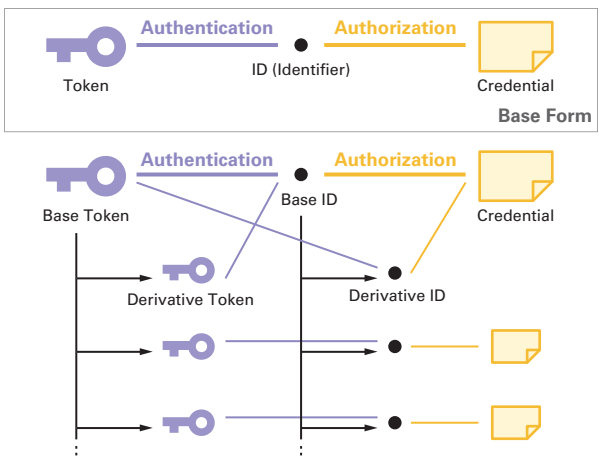


Figure 15: The Concept of Derivative Tokens and IDs

Agency published case studies regarding illegal remittances in Internet banking for 2014*58, indicating that over 100 financial institutions had incurred losses, and that damages were also on the increase. Particular attention was given to attacks targeting corporate accounts that involve comparatively large remittance amounts, and an alert was issued*59. In addition to methods that simply use a password, those that incorporate client authentication based on X.509 certificates (strong authentication) have also been introduced for corporate Internet banking authentication, and these are known to provide more security. However, when these digital certificates are used there have still been cases disclosed in which automatic transfers have been made from PCs or browsers infected with malware*60. This demonstrates that even authentication methods using SSL/TLS client certificates are not sufficient.

Based on these circumstances, an effort is being made to improve the authentication methods used in Internet banking systems. In the past, random number tables listed on paper or card were used, along with hardware devices that display a one-time password. This latter case is an authentication method in which a temporary password is input at the same time as the primary PIN number (a 4-digit number) that corresponds to the password used for authentication at ATMs, etc. Even if the primary PIN number leaked, use of a one-time password that is discarded each time reinforces the identity verification with particularly important processes, such as address changes or large remittances.

However, as shown by Man-in-the-Browser attacks*61 and MITM attacks, if banking system transaction details such as the destination account number or transfer amount are re-written, illegal remittances are possible even when a disposable one-time password is used. This demonstrates the problem of it being impossible for a user to explicitly confirm whether or not a transaction is legitimate based on the information shown in the browser alone, even if authentication methods are improved. There is an undeniable possibility that transactions may have actually been rewritten by an attacker. In response to this problem, progress is being made towards migrating to the use of hardware devices equipped with an input device.

In the past, measures featuring the combined use of hardware devices during authentication have also been adopted at a number of banking systems. However, because this hardware device was simply a one-time password generator with no input interface, it could only be used to identify whether the user has the correct token, which has nothing to do with the transaction at hand. In addition to the abovementioned use of X.509 certificates, corporate banking systems also incorporate secondary measures such as only accepting transactions from specific IP addresses and PCs. However, because it is possible that the transactions a user sees have been rewritten, there is no fundamental countermeasure for Man-in-the-Browser attacks. In other words, even with improved identity verification the countermeasures were ineffective.

In response, there were announcements from financial institutions in 2015 that they would start using one-time password cards. Unlike previous devices, these new hardware devices have a keypad input interface, enabling identity verification while also incorporating techniques that enable users to confirm the legitimacy of transactions that may have been rewritten. The devices are not merely for outputting the one-time password during authentication like before. They feature functions for generating and displaying one-time passwords that guarantee the correctness of account numbers, by having users themselves input the account number they want to transfer money to. This prevents money being sent to the account intended by an attacker, and by also recording the transaction log generated at this time, it is possible to automatically create blacklists for the attacker's accounts. Additionally, for user convenience, they can also be used as one-time password generators with no input device. The technique is based on the assumption that accounts registered by users in advance are safe, and omits the input of account numbers for transfers to these pre-registered accounts.

*58 National Police Agency, "Status of Incidents of Illegal Remittance Related to Internet Banking in 2014 (February 2015)" (http://www.npa.go.jp/cyber/pdf/H270212_banking.pdf) (in Japanese).

*59 IPA, "Have you implemented sufficient countermeasures for illegal remittances in corporate Internet banking? (August 2014)" (https://www.ipa.go.jp/files/000040703.pdf) (in Japanese).

*60 Trend Micro Security Blog, "Analyzing digital certificate theft attacks targeting corporate net banking" (http://blog.trendmicro.co.jp/archives/9417) (in Japanese).

*61 2nd Secure Systems Symposium - Hiromitsu Takagi and Hajime Watanabe, "The threat of Man-in-the-Browser and fundamental countermeasures" (https://www.risec.aist.go.jp/files/events/2014/0313-ja/risec-sympo2014-takagi.pdf) (in Japanese).

Now we will analyze the current state of these countermeasures. First of all, because only the account number is input, the legitimacy of the transaction amount cannot be guaranteed. For accounts that large numbers of users register, such as the account of an educational institution for receipt of tuition money, there is a possibility of business being obstructed by attacks that change the transaction amount during a specific short period of time. Secondly, there is the fact that the bank to transfer money to is not specified. In this case, if there was an account at another bank with the same account number under the control of the attacker, there would be a risk of illegal remittance taking place. Either way, the fact that users only explicitly confirm the account number is a problem. The more measures that are implemented, such as enabling users to explicitly check transfer amounts and bank codes for transactions, the more data that users will input into the device. Regarding this point, one potential solution is providing a range of options to select from based on how likely a user thinks it is that transactions will be rewritten. This is based on the same approach as having a user choose whether or not they permit the use of email addresses as IDs. With regard to this, it is also best to strike a balance between user convenience and security.

Additionally, a browser that implements FIDO Alliance's Second Factor UX*62 has come onto the scene. This is a standard that enables identity to be verified without entering a password, through use of a small hardware device via an interface such as USB. Its use has spread since last year. However, if it becomes more mainstream, the following points will also be of concern. Just as there are organizations that prohibit USB flash memory being brought on-site, the use of FIDO standard USB devices may be restricted. Consequently, it is possible that products such as IC card based devices that are always carried when entering rooms and require secure management like an employee ID card will appear. Currently, these identity verification methods are in a transitional period. We are approaching the day where other tokens will be required in addition to simply "something you know" like a password. This will include tokens categorized as "something you have" or "something you are". This is the dawn of an age in which users can select powerful identity verification systems for important communications by impairing convenience slightly.

1.4.3 Evaluating the IOCs of Malware That Reprograms HDD Firmware

On February 16, 2015, Kaspersky released information on an attack group called the Equation Group*63. The Equation Group use a variety of malware sets including EquationLaser, EquationDrug, DoubleFantasy, TripleFantasy, Fanny, and GrayFish. It could be said that one of their unique characteristics is the fact that they use a module for reprogramming hard disk drives (HDD) that is embedded as a plug-in in EquationDrug and GrayFish. Kaspersky states that the functions of this module can be used to sustain malware even after OS reinstallation or reformatting file systems. It is also able to generate invisible data areas on an HDD, making it harder to detect or delete malware. IIJ has analyzed the initial behavior of this module*64, and evaluated indicators of compromise (IOCs)*65 for detecting its presence in memory.

■ Overview of Initial Behavior

The module that reprograms HDD firmware ("nls_933w.dll") is loaded by a DLL called Platform Orchestrator (mscfg32.dll). After loading, mscfg32.dll calls a number of function addresses that nls_933w.dll exports, deobfuscates the character strings, and performs initialization such as the copying of function addresses on the mscfg32.dll side, before executing the function that carries out the main processing.

*62 The FIDO Alliance (https://fidoalliance.org/specifications/overview/).

*63 Kaspersky Lab's Global Research & Analysis Team (GReAT) published a report on the Equation Group. "EQUATION GROUP: QUESTIONS AND ANSWERS" (https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf).

*64 The MD5 hash value of the specimen is 11fb08b9126cdb4668b3f5135cf7a6c5.

*65 IOCs are traces indicating threats such as malware infections or incidents of compromise left behind on a network or device. See "1.4.2 The openioc_scan Plug-in That Scans for Threats Lurking in Device Memory" in Vol.26 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol26_EN.pdf) for more information about IOCs in memory.

A driver (win32m.sys) is first loaded from the resources in the function that carries out the main process of nls_933w.dll. Subsequently, win32m.sys is controlled via the DeviceIoControl API to confirm the module version, and initialization such as the clearing/setting of IO request handlers is carried out. If there are no issues, processing moves on to the queuing of IO requests for issuing ATA commands.

During this queuing process, a command (IDENTIFY DEVICE) for obtaining HDD information is first sent to win32m.sys. From the information obtained, details such as the serial number, firmware revision, and model number are checked, and then a further command (INITIALIZE DEVICE PARAMETERS) may be sent depending on the model number. After this, if it is determined from the HDD information that the target can be reprogrammed, a command (DOWNLOAD MICROCODE) related to firmware updates is sent.

■ Evaluation of IOCs

As we stated initially, nls_933w.dll makes it difficult to detect and delete malware from an HDD. However, because the API of this DLL is required to access the hidden data space, the same DLL must at least exist in memory. Consequently, based on the initial behavior detailed earlier, we will evaluate IOCs for detecting this DLL (and the drivers it loads) from a memory image.

First, we will look at IOCs specific to the detection of nls_933w.dll. IOCs that can be detected in both the DLL and the driver include IoControlCode, which is specified in the DeviceIoControl API. This malware uses the six IoControlCodes shown in Figure 16, and these can all be defined as IOCs using the AND condition.

Furthermore, defining the binary sequence comprised of the 6 byte structure in nls_933w.dll used to read and write ATA device registers is also effective if only applied to the detection of nls_933w.dll. This structure consists of register offsets and data to write, so for the command that obtains HDD information (IDENTIFY DEVICE), for example, the two binary sequence structures shown in Figure 17 (a total of 12 bytes) exist in memory. Additionally, the module contains many structures that include ATA commands, so these are defined using AND. Meanwhile, structures like these are not included on the driver side, but one method to use could be defining the code sequence that parses these structures.

Next, we will evaluate generic IOCs for detecting malware with similar behavior, not limited to nls_933w.dll. The first thing that comes to mind is the model numbers such as “Maxtor STM” and “WDC WD” that are used during the process of identifying HDD firmware. However, in the case of nls_933w.dll these are obfuscated, and after deobfuscation the strings are loaded onto the stack, so it could be said that they are difficult to find in valid memory space after the fact.

Other possible generic IOCs include the APIs used in the driver to read from or write to hardware ports or registers. For example, an API called WRITE_PORT_UCHAR is used to write to the ATA device registers described earlier, and similar APIs are also used based on the read or write size. It may be possible to detect drivers with functions like nls_933w.dll by defining the imported APIs such as these using AND. However, generic definitions like this will result in a higher likelihood of false positives occurring. Upon verifying detection using this definition with a number of 32-bit Windows XP and Windows 7 memory images, false positives occurred with a number of drivers on Windows 7*66. Consequently, we defined both the previously mentioned API group, as well as API groups related to other processing. Specifically, as shown in Figure 18, false positives can be eliminated by also defining APIs related to IO request queuing (thread generation, DPC queuing).

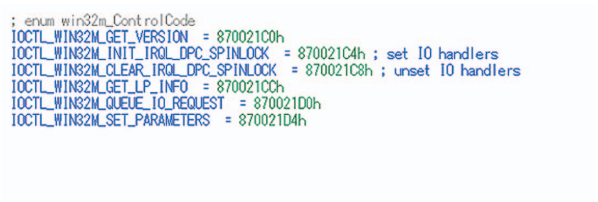


Figure 16: IoControlCode Used by nls_933w.dll

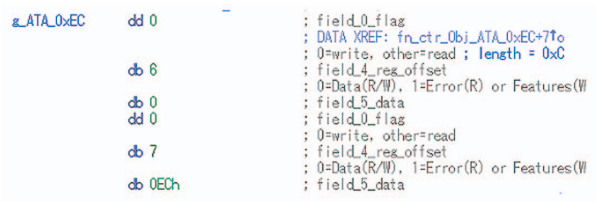


Figure 17: Structures for the Command that Obtains HDD Information (IDENTIFY DEVICE)

*66 The specimens we obtained were actually not designed to enable the loading of drivers in Vista or later environments with UAC enabled.

The presence or lack of the kernel timer function related to the abovementioned queue processing is another generic IOC that can be defined. Use of this definition alone is highly likely to result in false positives, so we recommend definition of the previously-mentioned API groups that are used via AND.

■ Summary

In this report, we demonstrated that there exist measures against malware that reprograms HDD firmware and hides data, showing that detection within memory can be effective. Here we evaluated IOCs especially for detecting this malware, as well as generic IOCs for detecting malware with similar functions*67. However, to produce results with fewer false positives in this latter case, it is necessary to create definitions that match the malware functions based on sufficient analysis and verification. As a result, it would be best to determine which approach to take as the occasion demands based on the urgency of response.

1.5 Conclusion

This report has provided a summary of security incidents to which IIJ has responded. In this report, we discussed increasingly malicious PUAs, examined ID management technology, and presented our evaluation of the IOCs for malware that reprograms HDD firmware. 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.

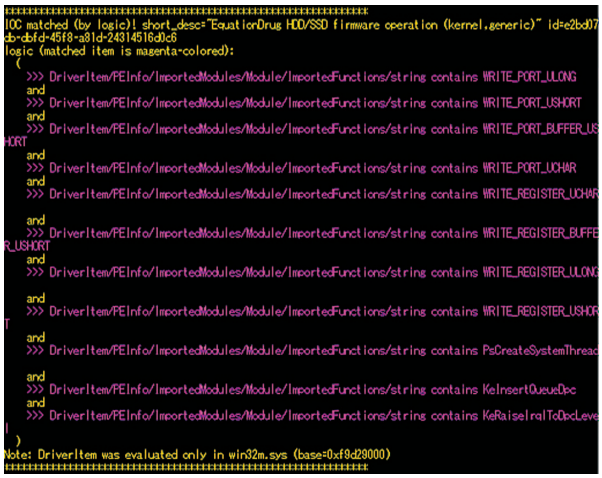


Figure 18: Detection Based on API Used

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, Tadaaki Nagao, Hiroshi Suzuki, Hisao Nashiwa (1.3 Incident Survey)
Hiroshi Suzuki (1.4.1 Increasingly Malicious PUAs)
Yuji Suga (1.4.2 ID Management Technology: From a Convenience and Security Perspective)
Takahiro Haruyama (1.4.3 Evaluating the IOCs of Malware That Reprograms HDD Firmware)
Office of Emergency Response and Clearinghouse for Security Information, Service Operation Division, IIJ

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

*67 The IOCs we discussed here are listed on the following site (https://github.com/TakahiroHaruyama/openioc_scan).

Anti-Spam Measure Technology and DMARC Trends

In this volume we report on spam trends incorporating the 52 weeks' worth of data from March 31, 2014, to March 29, 2015, while referencing data from IIR Vol.1.

Additionally, in our commentary on email technologies we discuss the RFC for DMARC that was authored recently, as well as the email framework for using DMARC, and the email ecosystem including domain reputation and feedback.

2.1 Introduction

In this report we discuss the latest trends in spam and email-related technologies, and examine a variety of anti-spam measures in which IIJ is involved. In "Spam Trends," we cover spam ratio trends since IIR Vol.1, including FY2014. We also discuss security topics arising from spam.

Under "Trends in Email Technologies," we take the opportunity to examine the benefits of introducing DMARC to aid it in becoming more widespread, in light of a DMARC RFC being authored. We also look at how sender authentication technology such as DMARC can be used effectively in email systems. We have already presented these concepts at events such as the Internet Association Japan's Anti-Spam Conference. In the future we would like to continue discussions in detail to work toward implementation, together with a number of organizations involved with anti-spam measures.

Last year, there were a number of events that became milestones for activities related to anti-spam measures. I will touch upon these at the end.

2.2 Spam Trends

In this section we examine spam trends, based on trends in the ratios of spam detected by the spam filter provided through IIJ's email services. Spam ratios are collated by week, because email usages rates differ for email users between weekdays and weekends. That said, spam ratios tend to be relatively higher on weeks that include long holidays such as the summer vacation and New Year periods, as the number of legitimate emails is significantly lower.

2.2.1 Spam Ratios Decline Further in FY2014

Figure 1 is a graph showing spam ratio trends for 356 weeks' worth of data from the initial IIR period (Vol.1, June 2008), including the 52 weeks between March 31, 2014, and March 29, 2015, which covers the year since the previous IIR (Vol.23). This indicates that average spam ratio for the past year (FY2014) was 31.7%. The average ratio stood at 47.4% the year before last (FY2013), so this represents a drop of 15.7%. The ratio of spam has fallen sharply since 2010, first remaining in the 40% range for some time with averages of 48.1% for FY2011 and 44.3% for FY2012, and now in FY2014 it has decreased further.

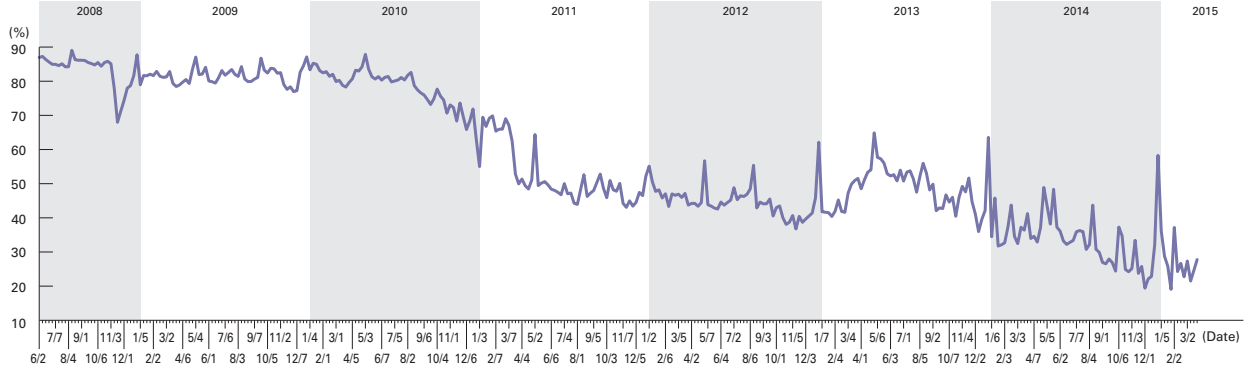


Figure 1: Spam Ratio Trends

Let us compare spam ratios over a longer period of time. The average ratio was 78.6% in FY 2009, so spam ratios, or in other words the volume of spam itself, has dropped considerably in the past five years. To give a more detailed explanation, because the ratio has fallen by 46.7%, if we were to suppose the number of standard, non-spam emails received remained constant over these five years, it would mean the overall volume of email received has fallen to a third of that before.

2.2.2 Higher Risks Despite Lower Volumes

These figures demonstrate that the volume of spam itself is on the decline, but as we have said in the past, it does not appear the risks that spam can pose have diminished. According to a report*1 published by the National Police Agency on February 12, 2015, there were 1,876 cases of illegal remittance in 2014, an increase over the previous year. Total damages came to 2,910 million yen, which is about double the 1,406 million yen in damages from the year before. Regarding the type of damages incurred, it was reported that there had been an increase in corporate bank accounts affected, rather than personal bank accounts. Regarding illegal remittance methods, it was reported that the technique of using viruses to automatically process illegal remittances was become increasingly sophisticated. This is thought to indicate that malware*2 is still being employed.

Let us examine how this kind of malware infiltrates the PCs of individuals and companies. Data on unauthorized access in the report*3 also published by the National Police Agency, among others, on March 19, 2015, listed two arrests for exploiting security holes, or in other words targeting vulnerabilities (security hole attacks in the report). Meanwhile, there were 336 arrests for the use of identification codes without permission. Of course, it is likely a considerable amount of malicious activity did not result in arrests, but from the data that we have at hand we can surmise that incidents exploiting vulnerabilities on a PC directly from an external source are (as yet) uncommon. These materials also listed the following points to note regarding defense against such incidents.

1. Appropriate configuration and management of passwords
2. Caution regarding phishing
3. Caution regarding malicious programs

Because the caution regarding phishing discussed taking care with email, it appears that email is being used to redirect users to phishing sites. Similarly, with regard to malware (malicious software), it was indicated that users should not open email attachments or files downloaded from untrustworthy websites. In short, we can see that email is used as a trigger for these malicious activities, and that accessing malicious sites listed in emails is a major cause of malware infections.

Regarding phishing, the Council of Anti-Phishing Japan*4 provides information such as lists of phishing sites that mimic actual websites and the sample phishing email text used to lure users to those sites. If you receive a suspicious email, we recommend you check whether it has been registered there. From a global perspective, APWG*5 publishes regular reports that I believe will prove useful for gauging recent trends.

2.3 Trends in Email Technologies

Here we will examine a variety of technological trends relating to email. This time we discuss the RFC for DMARC that was authored recently, as well as the email framework for using DMARC, and the email ecosystem including domain reputation and feedback.

2.3.1 The DMARC RFC

We have discussed the specifications of DMARC (Domain-based Message Authentication, Reporting, and Conformance) in this IIR since its origin and Internet-Draft ("I-D") stages. In March 2015, the core portions of DMARC were published as

*1 Status of Incidents of Illegal Remittance Related to Internet Banking in 2014 (http://www.npa.go.jp/cyber/pdf/H270212_banking.pdf) (in Japanese).
*2 Software created for certain malicious purposes, such as the theft of information, the sending of spam, or the processing of illegal remittances, is sometimes called malicious software or malware to differentiate it from the more widely-used term "viruses."
*3 Status of unauthorized access incidents and research and development for technology related to access control functions (https://www.npa.go.jp/cyber/statics/h26/pdf041.pdf) (in Japanese).
*4 Council of Anti-Phishing Japan (https://www.antiphishing.jp/) (in Japanese).
*5 APWG: Anti-Phishing Working Group (https://apwg.org).

RFC7489*6. Initially, the DMARC I-D was published and discussed as a standards-track item, but in the end it became an Informational RFC. I did not follow all the discussions of the IETF DMARC Working Group, so I am not fully aware of the reasons for it becoming an Informational, but it appears the change from I-D to Informational was made in April 2014.

As has been pointed out in the past, DMARC has an issue with authentication failing in a number of cases where use was normally possible. It is likely this issue had an impact during the standardization process, and it is also cited as a point requiring ongoing attention by the IETF DMARC Working Group. The issue originates from the fact that DMARC and the SPF and DKIM checks used as the basis for DMARC authentication each authenticate a different sender domain. We discussed this in Vol.16 of this report*7, which was published in August 2012.

2.3.2 Problems with DMARC and Reporting

One problem currently listed in the charter of the IETF DMARC Working Group as an issue that needs to be tackled is "indirect mail flows." Cases given as examples include the use of the following functions, which have been widely utilized as convenient email operations.

- Mailing list managers
- Automated mailbox forwarding services
- MTAs that perform enhanced message handling that results in message modification

In each case, the underlying cause is that the original email creator and the most recent sender from the perspective of the final recipient of that email are different, or that an intermediary function has changed the message. In April 2014, there was an actual incident in which U.S. company Yahoo! changed the DMARC record policy to "reject," resulting in the email of users participating in mailing lists via Yahoo! to fail DMARC authentication at delivery destinations from the mailing list. This caused receipt to be rejected according to the DMARC record policy. Meanwhile, after publishing that the DMARC record policy was to be changed to "reject," I heard from a staff member with a major U.S. bank who was pleased with the dramatic drop in complaints related to email that misrepresents its domain.

The goal of DMARC is to identify email that has the sender domain spoofed in this way, and prevent it from being delivered. However, to achieve this it is necessary to set the DMARC record policy to "reject." As shown in a previous example, this may have a significant impact. However, DMARC also features policies such as "none" and "quarantine," which are designed as transitions for a "reject" policy configuration. A domain administrator can configure policies with limited impact such as these, while utilizing the reporting function that reports authentication results to the sender. Based on this report, domain administrators can determine in advance whether authentication for legitimate email failed in any cases, and confirm about how many spoofed emails are in circulation to gauge the impact if the policy were to be changed to "reject." This kind of reporting is achieved by authenticating the sender domain for email received by the email recipient, and notifying the sender domain of information on email that fails authentication in the form of a report. Reporting is a new burden placed on the recipient side. However, to popularize the use of DMARC it will be necessary for more email recipients to provide this kind of reporting function.

2.3.3 Use of DMARC by Email Recipients

It could be said that from a sender's perspective there are significant advantages to DMARC, as publishing DMARC records prevents spoofed email from being delivered to the recipients. Then let us examine whether DMARC provides any benefits to recipients, who must add a new authentication function and report information on failed authentication to senders.

Up to now, we have stated a number of times that sender authentication technology such as SPF and DKIM are technologies for authenticating sender information, rather than for determining whether or not email is spam. This merely indicates that an authenticated sender domain has not been spoofed, so an authorization process is required to determine whether or not an email should be received. In the world of email, it has long been said that a reputation system for evaluating whether or

*6 Domain-based Message Authentication, Reporting, and Conformance (DMARC) (https://datatracker.ietf.org/doc/rfc7489/).

*7 "Messaging Technology 'Sender Authentication Technology Deployment and Authentication Identifiers'" in Vol.16 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol16_EN.pdf).

not email should be received based on the authenticated domain would be required to perform this authorization. DMARC enables a system in which domains are authenticated using SPF and DKIM, then ultimately DMARC, so it is at last possible to extract a domain using unified methodology. In other words, you could say it is now possible to perform an authorization process to determine whether or not to receive email using reputation based on individual domains.

Implementing DMARC benefits email recipients because clarifying the sender via sender authentication and evaluating them (the domain) reduces the number of unnecessary emails with a low reputation that should not be received. Preventing email recipients from receiving unnecessary email can lighten the load associated with a number of processes normally applied to received mail, such as virus checks and spam filter detection. It also means they do not need to be stored in the message spool. This reduces the burden of viewing and deleting unnecessary email for recipient users, too, improving user satisfaction.

2.3.4 Domain Reputation

The term "domain reputation" is still not clearly defined. In the past, there were examples of domains from which email should not be accepted being expressed as a domain blacklist, and conversely, domains from which email should be accepted were expressed as a whitelist. In general, domain reputation is thought of as a value that takes a more graded approach, rather than being limited to the two values of black or white (or three values if you including domains not included on either list).

For example, this makes it possible to automatically judge even domains with no clear data showing they had sent spam, based on information such as the amount of time that has passed since they were created, or the identity of administrators. That enables us to express their tendencies as a certain range. That said, to raise the accuracy of domain reputation, information on the authentication results of email actually received, and on detection of whether email is spam (or whether this is necessary) by the recipient is very helpful. Recently, I have seen records specifying domain names other than the corresponding one as the target for DMARC record reporting. It appears these reporting targets are also utilized as data for a company's own domain reputation by aggregating reporting emails, and collating cases in which DMARC authentication failed as a useful report, instead of providing them together. This demonstrates how it is possible for domain administrators and companies who collate reporting information to build a mutually beneficial relationship, so the number of businesses providing this kind of report analysis and reputation data may increase.

There are already cases of systems for reporting email received by a recipient as spam in Japan. For example, the Anti-Spam Consultation Center of the Japan Data Communications Association (JADAC) accepts information on spam by way of forwarded email or Web-based input. The Anti-Spam Consultation Center takes measures such as notifying the Ministry of Internal Affairs and Communications (MIC) if there are any violations indicated by this information. The MIC sends warnings to senders or implements administrative measures based on the information it has gathered*8.

If spam along with definitive sender information (domains) can be gathered using this system, it will be possible to further improve the accuracy of domain reputations. Until now, spam was sent to recipients in a one-sided manner, and the recipients had to exert effort individually to exclude it. However, once the use of DMARC becomes more widespread, and spam sender (domain) information can be aggregated over a wide area, enabling domain reputations to be provided as feedback, it may become possible to exclude unwanted spam in a more proactive manner.

*8 Ministry of Internal Affairs and Communications: Anti-Spam Measures (http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html) (in Japanese).

2.3.5 Email Ecosystems

Figure 2 is an overview (framework) showing the relationships between the DMARC implementation of sender authentication, the domain reputation evaluating authenticated domains, and the feedback reporting received email. This is an ecosystem that covers roles of each and sustainable systems for creating a better environment for email use, including the anti-spam measures we have discussed to date. Allow me to go over the basics of each role.

First, when email is received, domain authentication is performed using SPF and DKIM, as well as DMARC. At this stage, assuming the various issues can be resolved using technology, and DMARC authentication fails with the sender policy configured as reject, it may be possible to block receipt (from a technical perspective). Next, the received and authenticated domain is evaluated using domain reputation. If an authenticated domain is registered to a whitelist in advance, it can be delivered to the mail recipient without processing the spam filter, depending on the situation. The difficult aspect of spam filters is how to exclude clever spam that makes itself hard to identify. On the other hand, it is necessary to take measures to prevent false positives in which normal email that should be received is detected as spam. Email like this that is hard to detect based on its content alone can be delivered to recipients easily if the authenticated domain name is included in a whitelist.

Additionally, if it is known that an authenticated domain is clearly one that sends spam, it can be excluded easily without passing it through the spam filter. This shows that if the number of cases detectable in advance increases, it may also be possible to keep spam filter equipment costs in check.

We have reported cases in the past where IDs and passwords subject to SMTP authentication when mail was sent were exploited to use legitimate mail submission servers as stepping stones. To sum up, because the message passes over a legitimate email delivery route, even under this framework, spam would be delivered if that sender were registered to the whitelist. In this case, as long as the recipient can report the false negative (as feedback) to the sender managing domain reputation, it will be possible to detect the transmission server being used as a stepping stone. If the sender-side company references the SMTP authentication records for when an email is sent, it is possible to look up where that email was actually sent from, and who the physical sender is. For example, the PC may be infected with malware, or that subscriber may be explicitly sending spam, but in either case the source of the email can be confirmed, so measures can be taken.

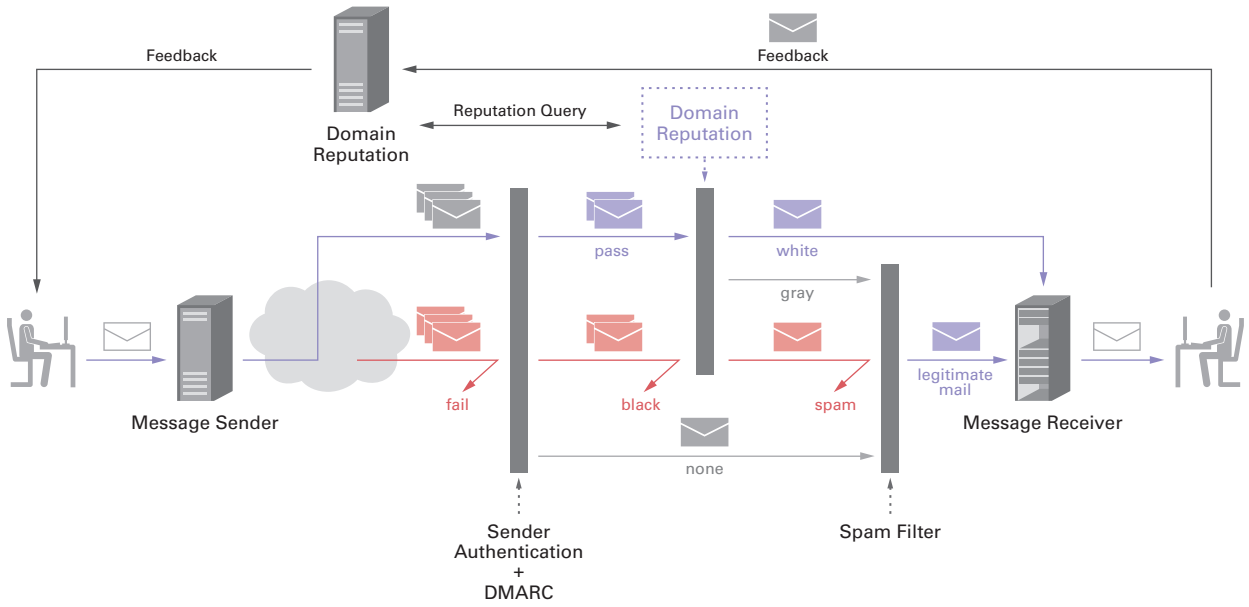


Figure 2: Email Ecosystem

2.4 Conclusion

Last year, in October 2014, the 10th annual conference of the London Action Plan (LAP*9), LAP 10 Tokyo was held at Keio Plaza Hotel in Tokyo. LAP is an organization that brings together administrative agencies from various countries involved with anti-spam measures, and there are currently 27 countries participating. From Japan, the Ministry of Internal Affairs and Communications (MIC) and the Consumer Affairs Agency take part as members. This is closely related to the M³AAWG that I am a member of, and as we have previously held joint meetings on occasion, for the past few years I have taken part in independent LAP meetings together with MIC members. Past LAP conferences have only been held in Europe or North America, but last year the 10th annual conference took place in Japan, the first time it has been held in Asia. To build up this milestone conference, the Anti-Spam mail Promotion Council (ASPC) that I belong to formed a committee to prepare for the LAP 10 Tokyo conference. We put together a panel exhibition at an adjoining exhibition hall, and held the Internet Association Japan's Anti-Spam Conference at the same venue, with the aim of encouraging the general public to attend as well. During the LAP conference I also gave a presentation on the anti-spam measure activities carried out in Japan to date, as a representative of the ASPC. Thanks to the efforts of many contributors, the LAP 10 Tokyo conference ended in success, and participants also voiced their approval of how it turned out.

M³AAWG, which was established in 2004, also reached its 10-year milestone last year. The 32nd General Meeting was held in October 2014 in Boston, USA, the same place where I took part in the initial Founding Meeting. To commemorate the 10th anniversary, the original agenda was presented at the opening, and speeches were given by the three members who have taken part in the most conferences, including me.

When administrative agencies and private organizations came together 10 years ago, I had no inkling that our anti-spam measure activities would still be ongoing a decade later. We launched JEAG*10 in Japan in 2005, and if you include its predecessor organization, 10 years have passed since then. This was another activity I did not expect to last so long at first. I didn't think the problem of spam would be so protracted. For that reason, JEAG was not set up as a formal organization, and everyone involved with it has acted as a volunteer all this time. Still, there is no way a group like that can sustain itself forever, and it has pretty much run its natural course, but the purpose of these activities and the importance of organizations such as these appear to remain unchanged 10 years on. That may be because the system known as email has grown in importance, transforming from a supplementary tool that only a few use into one of the foundations of society.

Naturally, I believe it would be best if these anti-spam measures were no longer needed one day, but at this point in time that may be difficult. I would like to at least help develop an environment where email can be used with a little more peace of mind.

Author:

Shuji Sakuraba
Mr. Sakuraba is a Senior Engineer in the Service Development Section No.2 of the Application Development Department of the IIJ Product Division. He is engaged in the research and development of communication systems. He is also involved in various activities in collaboration with external related organizations for securing a comfortable messaging environment. He has been a member of M³AAWG since its establishment. He is acting chairperson of the Anti-Spam mail Promotion Council (ASPC) and a member of its administrative group, as well as chief examiner for the Sender Authentication Technology Workgroup. Additionally, he is a member of Internet Association Japan's Anti-Spam Measures Committee.

*9 London Action Plan (http://londonactionplan.org).
*10 JEAG: Japan Email Anti-Abuse Group (http://jeag.jp) (in Japanese).

Report on Access Log Analysis Results for Streaming Delivery of the 2014 Summer Koshien

In live streaming of the National High School Baseball Championship held at Koshien Stadium (Summer Koshien) in August 2014, peak traffic of 108 Gbps was recorded, and there were approximately 1.9 billion requests. Here we examine the scale of access, as well as differences in access trends based on device types, as revealed by the results of analyzing the logs of all delivery servers.

3.1 Overview of Streaming Delivery of the 2014 Summer Koshien

IIJ provides streaming delivery services for Summer Koshien, which is produced by Asahi Broadcasting Corporation*1. Every year the special website set up by Asahi Broadcasting Corporation gets large numbers of hits, with most involving the receipt of live streamed content. Peak traffic of 108 Gbps was recorded during the final of the 2014 Summer Koshien on August 25, 2014.

In 2014, 38 Web servers were used for the live streaming of Summer Koshien (Figure 1). Asahi Broadcasting Corporation encodes the video, then uploads it to the ingest servers at IIJ using RTMP (Real Time Messaging Protocol). The ingest servers generate two types of content: HLS (HTTP Live Streaming) for mobile devices, and HDS (HTTP Dynamic Streaming) for PCs. These two types of content are cached on the web servers that act as the front end for clients, and the web servers return the requested content in response to requests from each client.

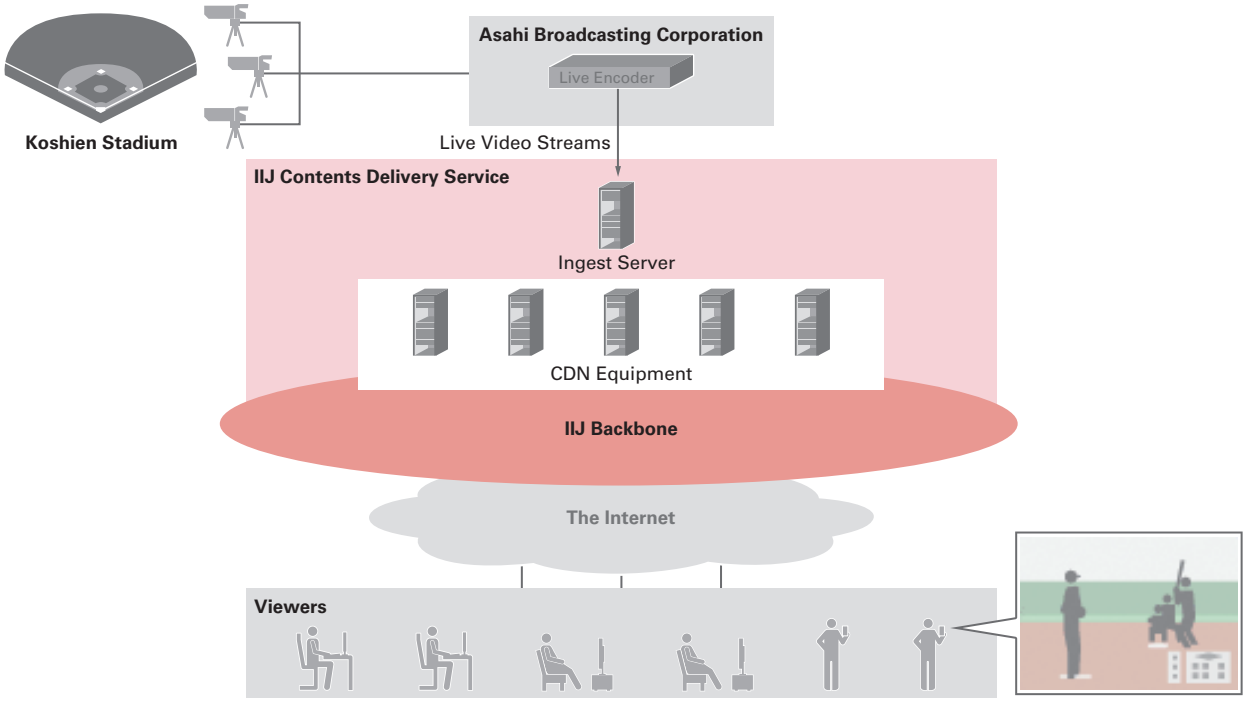


Figure 1: Conceptual Diagram for Delivery System

*1 Refer to Vol.25 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol25_EN.pdf).

While watching a live stream, the client (a browser for PCs, or a dedicated application for mobile devices) downloads a playlist and segment files repeatedly. The playlist contains a list of segment files that can be downloaded at the current point in time, while the segment files contain video that is split into fixed intervals of time. Unlike the playback of long video files, clients must play back consecutive short segment files one after another to display a live stream. That means they must refer to a continually updated playlist and download segment files repeatedly to perform playback.

These repeated client requests for playlist and segment files are recorded along with the time of requests in access logs on each Web server. Because a large amount of access is concentrated in Summer Koshien live streaming, these access logs end up at the massive size of around 1.9 billion lines. The access logs contain a large number of records related to actual viewing activities of users, so by analyzing them we can understand the current state of user viewing trends and viewing quality in a production environment. We would like to utilize the knowledge we gained to improve the quality of streaming delivery in the future.

Table 1 indicates the scale of access for the live streaming of the 2014 Summer Koshien. The values shown here are calculated based on the access logs for all Web servers over the entire duration of the championship. The total number of requests matches the number of lines in the access logs mentioned earlier. The total amount of content sent is the total file size of each piece of playlist and segment file content recorded in the access logs. When content is sent from Web servers, headers for various protocols such as HTTP, TCP, and IP are also included. As a result, the volume of data sent from the Web servers actually exceeds the total amount of content sent.

There were 1.3 million unique IP addresses, and we found that a little over half of these (55%) were from mobile devices. This was the first time Asahi Broadcasting Corporation officially supported mobile devices by providing dedicated mobile applications for Summer Koshien live streaming, and it is now clear that many users actually viewed the live stream using mobile devices. When multiple clients receive live streaming via NAT, to Web servers it is seen as access from the same IP address, so in this case it is counted as a single unique IP address.

Table 1: Scale of Access for Live Streaming of the 2014 Summer Koshien

Total number of requests (hundred millions)	19.73
Total amount of content sent (TB)	531.4
Number of TCP connections (hundred millions)	2.81
Number of unique IP addresses (millions)	1.30

3.2 Changes in Access Numbers by Day and Hour

The 2014 Summer Koshien was postponed for two days due to rain, so it was held between August 11 (Mon) and August 25 (Mon), including a rest day on August 23 (Table 2). Usually, client numbers tend to increase as the championship progresses to the semifinals and final. To examine whether 2014 followed this pattern, we will first look at changes in access numbers during the championship based on the number of requests by day and hour.

Figure 2 shows changes in the number of hits by day. This bar graph indicates the number of hits per day. Before and after August 18, the trend in daily access numbers varies. Prior to August 18, the number of hits was lower overall, while for the following five days they were much higher. One plausible reason for the lower access numbers before August 18 is the Bon Festival that fell between August 13 and August 15. During this period many people took their summer vacation and were watching the Summer Koshien broadcast on TV at home, resulting in a decrease in live streaming views. The growth in the number of hits after the Bon Festival on August 18 and beyond is thought to be because people who were unable to watch the TV broadcast of the event during the week were watching via live streaming.

Next, Figure 3 shows changes in access numbers by hour. While Figure 2 showed the number of hits for each day, Figure 3 shows the number of hits per day divided into hourly increments. The number of requests on the day of the final is remarkable. The peak traffic was recorded on August 25 when the final was held, and at the same timing, the peak number of requests by hour was recorded. On the 25th the only game held was the final from 1:00 PM, and the high number of requests for the final is clearly demonstrated by the fact that request numbers by hour were more than double those for other game days.

Table 2: Schedule Overview for the 2014 Summer Koshien

Dates	Game Summary
August 11 (Mon) - August 14 (Thu)	Game 1
August 15 (Fri) - August 19 (Tue)	Game 2 (Game 1 for the first game on August 15 only)
August 20 (Wed) - August 21 (Thu)	Game 3
August 22 (Fri)	Quarterfinals
August 23 (Sat)	Rest day
August 24 (Sun)	Semifinals
August 25 (Mon)	Final

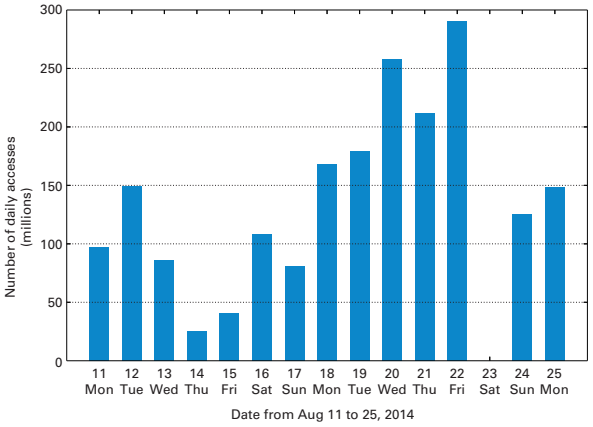


Figure 2: Changes in the Number of Hits by Day

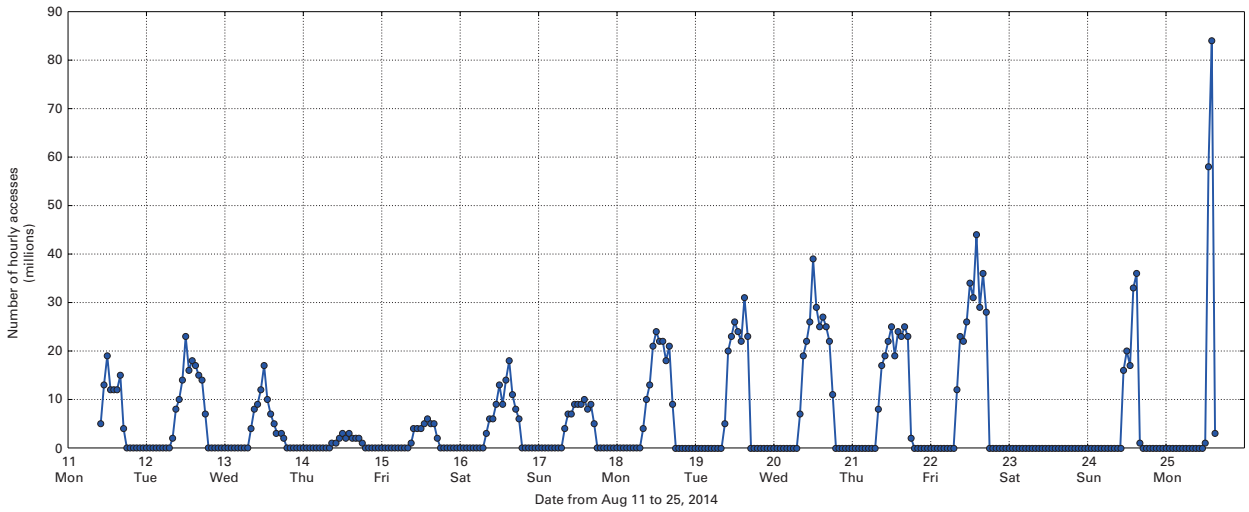


Figure 3: Changes in the Number of Hits by Hour

3.3 Differences in Viewing Activities by Device

Because this was the first trial of live streaming entire games for mobile devices, we will also examine differences between the viewing activities on PCs and mobile devices. Here we focus on the viewing time and viewing length.

3.3.1 Differences in Viewing Time

It is thought that viewing times vary for PCs and mobile devices such as smartphones because of differences in device usage. The first thing that comes to mind is that higher mobile device usage is expected during the times of day when people commute to work or school. Let us see if there were differences in viewing times based on device for the live streaming of Summer Koshien.

During the championship, there was some variance in the number of games held each day as well as the start time for games. If the numbers of games and start times are different, it is more likely that user viewing patterns will also change. For this reason, we selected eight days in which games were held from 8:00 am (August 13 - 14, 16 - 18, and 20 - 22), so we could target days where games took place around the same time of day. Of these eight days, six were weekdays, and the remaining two days fell on the weekend.

Using the access logs for these periods, we identified the number of requests by device for each hour between 8:00 am and 6:00 pm, and from this we calculated the proportion of access from mobile devices by hour. Figure 4 shows a box plot indicating the results of aggregating access ratios for each hour over the eight day period. The upper and lower parts of the blue boxes in the graph indicate the 75th percentile and 25th percentile, respectively. The red line in the boxes shows the median of the distribution. The median value for the 8:00 am timeslot was 71.8%, showing how high access from mobile devices was. The median value was 50% in the 9:00 am timeslot that followed, indicating that mobile devices accounted for half of the access numbers. After 10:00 am the median value fell below 40%, and continued fluctuating around 30%.

These results suggest that many users viewed the live streaming of Summer Koshien on mobile devices during the work and school commute period. After office hours began, users appeared to shift to viewing from PCs.

3.3.2 Differences in Viewing Length

The viewing time isn't the only aspect that differs between PCs and mobile devices. It is also conceivable that viewing length will vary. In the past, prolonged viewing of streaming video on the move was difficult for a number of reasons, such as the small screen size of mobile devices, and the lack of network bandwidth while mobile. However, there are now smartphones with large screens in addition to tablets, and the bandwidth available to mobile network environments has increased due to LTE and offloading to Wi-Fi. As a result, we are approaching the point where extended viewing from mobile devices is possible.

For comparison between the lengths of viewing on PCs and mobile devices, it is necessary to extract request sequences for each view from the access logs, and compare their lengths. However, user and viewing identifiers are not recorded in the access logs. Consequently, as an alternative we decided to shed light on trends in viewing length between PCs and mobile devices by comparing the length of consecutive segment file numbers.

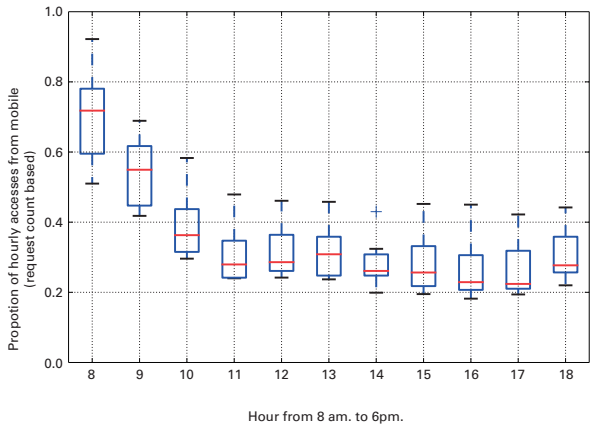


Figure 4: Hourly Mobile Device Access Ratios

Specifically, from access logs classified by client IP address and device type, we extracted only the segment file requests, then we identified places where there were five or more consecutive segment numbers in a request sequence. After this, we compared these numbers of consecutive segment files. We limited our research to places with five or more consecutive segment numbers, because it would not be appropriate to count places where the number of

segment files was too small to consider viewing. Due to the use of a method like this, we should make it clear that the number of segment files does not indicate the viewing time of each user.

Figure 5 shows the cumulative frequency distribution for the number of consecutive segment files on PCs and mobile devices. Comparing the number of consecutive segment files on PCs and mobile devices, those for PCs are around twice as long as those for mobile devices. Additionally, comparing median values we can see that those for PCs are 2.5 times longer than those for mobile devices. These results demonstrate that viewing length tends to be longer on PCs than on mobile devices. Furthermore, based on client-side measurement of viewing time, on PCs viewing time was about 20 minutes, while for mobile devices the viewing time was around 10 minutes. These results also point to viewing length being longer on PCs than on mobile devices.

3.4 Comparison of Client Numbers and Access Numbers by Device

In the previous section, we examined differences in viewing time and viewing length for PCs and mobile devices. Here we look into differences between PC and mobile device usage methods a bit further, based on the number of clients and hits.

Figure 6 shows daily changes in the number of clients for PCs and mobile devices, while Figure 7 shows daily changes in the number of hits from them. The two figures compare PCs and mobile devices day-to-day, but each indicates a different trend.

First, looking at the number of clients in Figure 6, we can see that the number of mobile device clients exceed the number of PC clients on almost all game days. Even on days where this wasn't the case, the number of mobile device clients was almost on par with the numbers for PC. Meanwhile, Figure 7 shows that the number of hits from PCs exceeded those from mobile devices on all game days.

As you can see, when we compare the number of clients and hits for PCs and mobile devices, mobile devices had high numbers in one case, and PCs in the other. This can be explained by the differences in the number of hits per client on PCs and mobile devices.

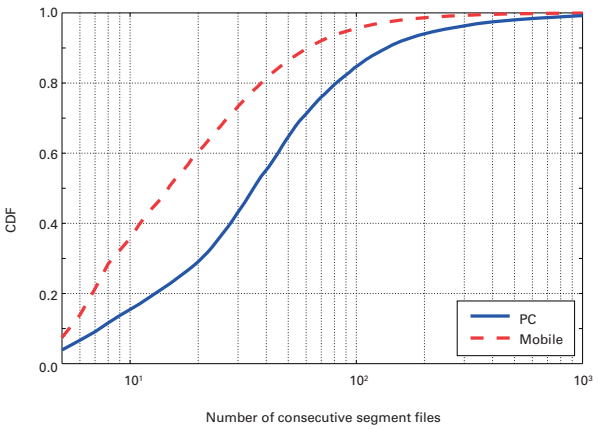


Figure 5: Number of Consecutive Segment Files Distribution by Device Type

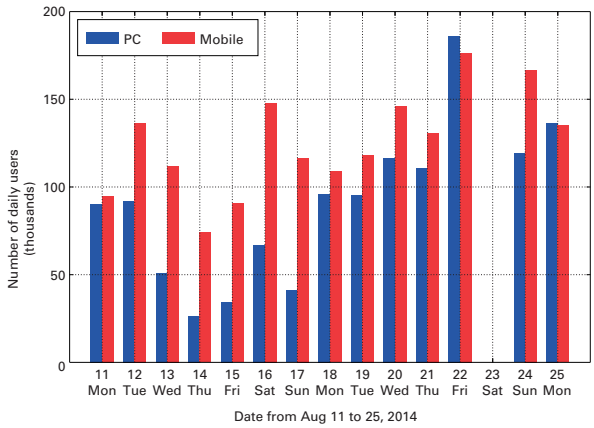


Figure 6: Comparison of Daily Client Numbers by Device

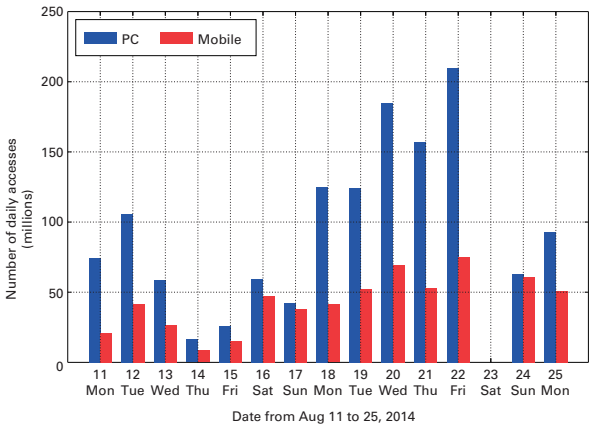


Figure 7: Comparison of Daily Access Numbers by Device

Figure 8 shows the cumulative frequency distribution for daily requests per client on PCs and mobile devices. Games took place for over 10 hours a day in longer cases, and if all 10 hours of streaming were viewed, a total of 4,500 segment files would be downloaded. Meanwhile, in Figure 8, PCs and mobile devices both converge on 1.0 around 5,000 where the green line is drawn. This suggests that although the ratio is small, some clients continued playback of video streaming for almost the full day.

Comparing the distribution of hits for PCs and mobile devices in Figure 8, we can see the access number distribution for each diverges from just after 10. The average for PCs is around 610 per client, while for mobile devices the average is around 158 per client, meaning access from mobile devices is only about a quarter that on PC. By understanding the extent of the difference in access numbers for each client on PCs and mobiles devices, we can comprehend that, even when the number of clients for mobile devices are higher than those for PCs in the abovementioned Figure 6, the number of hits for mobile devices are lower than those for PCs in Figure 7.

3.5 Conclusion

From the results of our investigation into live streaming for the 2014 Summer Koshien based on access logs for all delivery servers, we have seen changes in the scale and size of access, and identified differences in the access trends for PCs and mobile devices.

This was our first attempt at live streaming entire games to mobile devices via streaming delivery, and the analysis results revealed some differences in viewing trends between PCs and mobile devices. Examples include the fact that a particularly large number of viewers use mobile devices during the time when people commute to work and school, and the fact that mobile device viewers watch for shorter periods than PC viewers. Because the trend toward viewing streaming from mobile devices is set to accelerate in the future, we consider it crucial to analyze mobile device usage trends during the course of actual service to understand the viewing quality experienced.

Although we did not have the opportunity to discuss them this time, we are also conducting surveys and analysis based on the access logs used here with regard to viewing quality, including client behavior while viewing. We will continue performing surveys and analysis like this in the future, to help improve the quality of streaming delivery services.

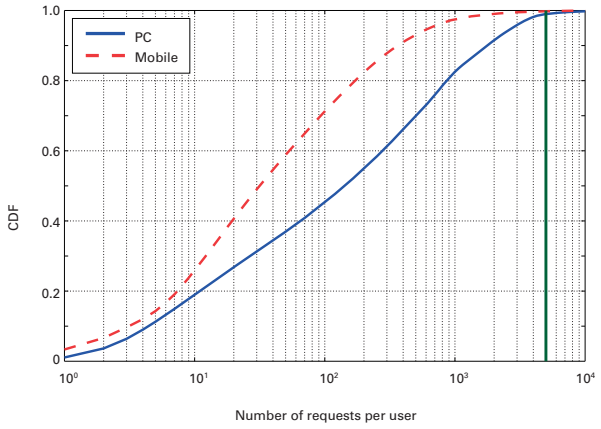


Figure 8: Access Number Distribution for Each Client by Device

Author:

Megumi Ninomiya
Ms. Ninomiya is a researcher at the Research Laboratory of the IIJ Innovation Institute. She is involved in research into Web traffic.

Vol.27 May 2015

About Internet Initiative Japan Inc. (IIJ)

IIJ was established in 1992, mainly by a group of engineers who had been involved in research and development activities related to the Internet, under the concept of promoting the widespread use of the Internet in Japan.

IIJ currently operates one of the largest Internet backbones in Japan, manages Internet infrastructures, and provides comprehensive high-quality system environments (including Internet access, systems integration, and outsourcing services, etc.) to high-end business users including the government and other public offices and financial institutions.

In addition, IIJ actively shares knowledge accumulated through service development and Internet backbone operation, and is making efforts to expand the Internet used as a social infrastructure.

Internet Initiative Japan Inc.
Address: Iidabashi Grand Bloom, 2-10-2 Fujimi, Chiyoda-ku, Tokyo 102-0071, Japan
Email: info@iij.ad.jp URL: http://www.iij.ad.jp/en/

IIJ-MKTG020YA-1506CP-00001PR