# Countermeasures Against the Alteration of Domain Name Registration Information

**In this report, we discuss countermeasures against the alteration of domain name registration information, and examine the openioc_scan plug-in that scans for threats lurking in the memory of a computer. We also take a look at ID management technology.**

## 1.1 Introduction

This report summarizes incidents to which IIJ responded, based on general information obtained by IIJ itself related to the stable operation of the Internet, information from observations of incidents, information acquired through our services, and information obtained from companies and organizations with which IIJ has cooperative relationships. This volume covers the period of time from October 1 through December 31, 2014. In this period a number of hacktivism-based attacks were once again carried out by Anonymous, and a series of targeted attacks on companies such as media outlets were discovered. There were also incidents of suspicious messages being displayed as well as malware infections originating from alterations and domain hijackings caused by attacks on domain name registries, with companies in Japan also being affected. In November, there was an incident in which a movie-related company in the United States had its corporate IT system rendered inoperable. A large quantity of information was also stolen, and some of this was released to the public. 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 October 1 and December 31, 2014. Figure 1 shows the distribution of incidents handled during this period*1.

### 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 incidents and causes. In October there were a number of defacements and information leaks affecting websites of the Chinese government and the Hong Kong executive branch in relation to demonstrations in Hong Kong (OpHongKong). In November, the websites of a number of government institutions in the Philippines were defaced in protest against the government. In Turkey, the website of a power transmission company was compromised by a party protesting against the Turkish government. There

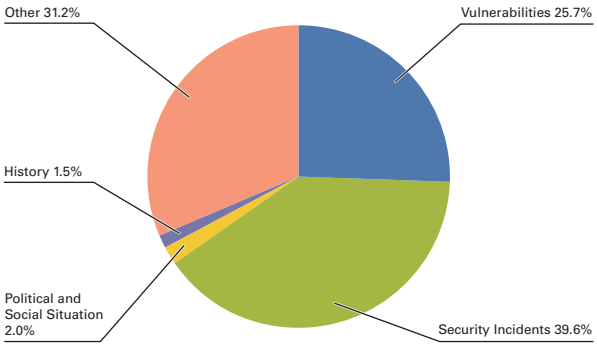



**Figure 1: Incident Ratio by Category (October 1 to December 31, 2014)**

*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.

were also a number of website defacements and compromises in Turkey thought to be the work of another party. Attacks continue to be made on a number of sites for the Israeli government and private-sector businesses in relation to the conflict in Palestinian-controlled Gaza Strip. Similarly, attacks related to conflict were also made between countries such as Russia and Ukraine, Pakistan and Indonesia, and India and Pakistan. 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 companies such as media outlets.

### ■ Vulnerabilities and their Handling

During this period fixes were released for Microsoft's Windows*2*3*4*5, Internet Explorer*6*7*8, and Microsoft Office*9. In December, a lot of interest was generated when Google disclosed a vulnerability*10 it had discovered in Windows 8.1 Update with no fix available. This was due to Google's policy of automatically disclosing vulnerability information 90 days after it is reported in some cases, but some expressed concern at Google making this information public*11. Updates were also made to Adobe Systems' Flash Player, Reader, and Acrobat. A vulnerability in JustSystems Corporation's Ichitaro that could allow execution of arbitrary program code by a third party was discovered and fixed. 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. An SQL injection vulnerability was also discovered and fixed in the Drupal CMS. A number of vulnerabilities, including an XSS vulnerability, were fixed in WordPress as well. Cases in which these vulnerabilities were exploited to actually steal administrative privileges have been confirmed*12. A vulnerability that could allow an external party to cause abnormal operations on a server or stop a service has been fixed in several pieces of DNS software, such as BIND and Unbound. A vulnerability that could allow arbitrary code execution with ntpd execution privileges using specially-crafted packets was discovered and fixed in the ntpd program used for time synchronization.

In October, a new method for attacking the SSLv3 protocol used with SSL/TLS servers called the POODLE attack (Padding Oracle On Downgraded Legacy Encryption attack) was disclosed*13. Because this vulnerability was caused by issues in the specifications of the protocol itself, the measures taken included fixes to disable SSLv3 in major Web browsers and servers, and the release of information on how to configure settings to prevent SSLv3 communications.

### ■ Attacks on Domain Name Registries

During this period, there were a number of incidents in which registration information at domain name registries and registrars was illegally altered in attacks, resulting in the redirection of users to malicious sites. In October, the PANDI ccTLD registry that manages Indonesia's .id domains was compromised, and visitors to Google's local site were redirected to another site. On a major video-sharing website it was confirmed that fake ads were used in attacks that attempted to infect

*2 "Microsoft Security Bulletin MS14-058 - Critical: Vulnerabilities in Kernel-Mode Driver Could Allow Remote Code Execution (3000061)" (https://technet.microsoft.com/library/security/ms14-058).

*3 "Microsoft Security Bulletin MS14-060 - Important: Vulnerability in Windows OLE Could Allow Remote Code Execution (3000869)" (https://technet.microsoft.com/library/security/ms14-060).

*4 "Microsoft Security Bulletin MS14-064 - Critical: Vulnerabilities in Windows OLE Could Allow Remote Code Execution (3011443)" (https://technet.microsoft.com/library/security/ms14-064).

*5 "Microsoft Security Bulletin MS14-066 - Critical: Vulnerability in Schannel Could Allow Remote Code Execution (2992611)" (https://technet.microsoft.com/library/security/ms14-066).

*6 "Microsoft Security Bulletin MS14-056 - Critical: Cumulative Security Update for Internet Explorer (2987107)" (https://technet.microsoft.com/library/security/ms14-056).

*7 "Microsoft Security Bulletin MS14-065 - Critical: Cumulative Security Update for Internet Explorer (3003057)" (https://technet.microsoft.com/library/security/ms14-065).

*8 "Microsoft Security Bulletin MS14-080 - Critical: Cumulative Security Update for Internet Explorer (3008923)" (https://technet.microsoft.com/library/security/ms14-080).

*9 "Microsoft Security Bulletin MS14-081 - Critical: Vulnerabilities in Microsoft Word and Microsoft Office Web Apps Could Allow Remote Code Execution (3017301)" (https://technet.microsoft.com/library/security/ms14-081).

*10 This vulnerability was fixed in January 2015 with "Microsoft Security Bulletin MS15-008 - Important: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (3019215)" (https://technet.microsoft.com/library/security/ms15-008).

*11 For example, problems were pointed out in the following SOPHOS nakedsecurity blog post. "Zero-day in Windows 8.1 disclosed by Google" (https://nakedsecurity.sophos.com/2015/01/03/zero-day-in-windows-8-1-disclosed-by-google/).

*12 For example, with Drupal an alert was issued due to the fact that attacks had begun a few hours after the fix was released on October 16. "Drupal Core - Highly Critical - Public Service announcement PSA-2014-003" (https://www.drupal.org/PSA-2014-003).

*13 See "1.4.2 The POODLE Attack" in Vol.25 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol25_EN.pdf) for more information.

## October Incidents

1 2 3 O **4th:** The Federal Communications Commission (FCC) ordered a major hotel chain to pay a $600,000 fine for intentionally blocking the Wi-Fi communications of customers and promoting their paid Wi-Fi system.
"Marriott to Pay $600K to Resolve WiFi-Blocking Investigation"
(http://www.fcc.gov/document/marriott-pay-600k-resolve-wifi-blocking-investigation-0). Regarding this issue, a warning was issued in January once again calling for business operators to not intentionally block tethering using Wi-Fi routers or smartphones. "WARNING: Wi-Fi Blocking is Prohibited" (http://www.fcc.gov/document/warning-wi-fi-blocking-prohibited).

4 S **5th:** An incident occurred in which the PANDI ccTLD registry for Indonesia's .id domains was accessed by an unknown party without authorization, and Google's site was hijacked.

5 S **10th:** U.S. security company Volexity reported that cyber attacks were occurring in relation to demonstrations in Hong Kong. Among these, it was identified that a number of sites in Japan, including the Web server of a Japanese newspaper publisher, had been altered to act as malicious sites or redirect users to malicious sites.
See the following blog post for more information: "Democracy in Hong Kong Under Attack" (http://www.volexity.com/blog/?p=33).

6 7 8 S **10th:** It came to light that data such as customer credit card information had leaked from a number of U.S. retailers due to malware.
For example, it is reported that the store payment system at major discount chain Kmart had been infected with malware. Sears Holdings Corporation "Kmart Investigating Payment System Intrusion" (http://searsholdings.mediaroom.com/index.php?s=16310&item=137317).

9 10 O **10th:** The JPCERT Coordination Center issued an alert due to an increase in scans to TCP port 10000, which is used by the Webmin Web-based system administration tool.
"JPCERT/CC Alert 2014-10-10 Alert regarding increase in scans to TCP port 10000" (http://www.jpcert.or.jp/english/at/2014/at140038.html).

11 12 13 14 15 V **15th:** Microsoft published their Security Bulletin Summary for October 2014, and released a total of eight updates, including three critical updates such as MS14-056 and MS14-058, as well as five important updates such as MS14-060.
"Microsoft Security Bulletin Summary for October 2014" (https://technet.microsoft.com/library/security/ms14-oct).

V **15th:** Oracle released their quarterly scheduled update for a number of products including Oracle, fixing a total of 154 vulnerabilities, including 25 in Java SE.
"Oracle Critical Patch Update Advisory - October 2014" (http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html).

V **15th:** Google disclosed the new POODLE (Padding Oracle On Downgraded Legacy Encryption) method for attacking the CBC cryptographic algorithm used by SSL 3.0.
See the following article from the Cryptographic protocol Evaluation toward Long-Lived Outstanding Society (CELLOS) for more information:
"[2014-10-15] On a new attack on SSLv3 specification called POODLE attack"
(https://www.cellos-consortium.org/index.php?PoodleAttack_20141015).

16 V **15th:** 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/apsb14-22.html).

17 S **15th:** Security warnings caused by Google Safe Browsing were displayed on some websites that featured a Hatena Bookmark button.
Hatena Bookmark Development Blog, "Regarding security warnings on some sites featuring a Hatena Bookmark button"
(http://bookmark.hatenastaff.com/entry/2014/10/18/021046) (in Japanese).

18 19 20 V **16th:** An SQL injection vulnerability (CVE-2014-3704) was discovered and fixed in the Drupal CMS application.
"SA-CORE-2014-005 - Drupal core - SQL injection" (https://www.drupal.org/SA-CORE-2014-005).

S **16th:** Trend Micro issued an alert due to the confirmation of attacks that redirect users to a malware distribution site from fake ads on YouTube.
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/).

21 22 23 O **17th:** The Ministry of Economy, Trade and Industry compiled and published its "Guidelines concerning the Online Services for Consumers regarding Notification on the Use of Private Data and Gaining Approval from the Consumer for Data Usage," to serve as reference for companies offering services overseas.
"Announcement of guidelines for providing information and explanations in consideration of the privacy of consumers on online services"
(http://www.meti.go.jp/press/2014/10/20141017002/20141017002.html) (in Japanese).

24 O **17th:** The National Police Agency issued an alert due to an increase in SSDP reflection attacks.
"Alert regarding SSDP reflector attacks using UPnP compatible network devices as stepping stones"
(http://www.npa.go.jp/cyberpolice/detect/pdf/20141017.pdf) (in Japanese).

25 26 O **21st:** Apple released a statement regarding issues with the Spotlight search function in OS X Yosemite sending user's current location and search information to them.
"OS X Yosemite: Spotlight Suggestions" (http://support.apple.com/kb/PH18943?viewlocale=en_US).

27 28 V **22nd:** Microsoft announced there was a vulnerability in Microsoft OLE (CVE-2014-6352) without a fix available that could allow remote code execution.
"Microsoft Security Advisory 3010060 Vulnerability in Microsoft OLE Could Allow Remote Code Execution"
(https://technet.microsoft.com/library/security/3010060). This vulnerability was fixed in "Microsoft Security Bulletin MS14-064 - Critical: Vulnerabilities in Windows OLE Could Allow Remote Code Execution (3011443)" (https://technet.microsoft.com/library/security/ms14-064).

29 30 31 O **31st:** The Ministry of Internal Affairs and Communications made an announcement regarding their initiatives to improve the mobile usage environment, such as removing SIM locks, promoting MVNOs, and allocating frequency spectrum for 4G and other high speed communications. The goal of these initiatives is to stimulate the economy and reduce the national burden through the creation of new mobile-based business.
"Announcement of Mobile Recreation Plan"
(http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/141031_05.html).

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

*Dates are in Japan Standard Time

users with ransomware. In this incident, it was identified that the attackers somehow altered the DNS information of the Polish government's domain and made it appear as a legitimate site. Incidents in which attempts were made to redirect users to malicious sites or infect certain users with malware have also occurred at major newspaper publishers and SNS services in Japan, with the cause thought to be the unauthorized alteration of domain name registration information. A U.S. security firm has reported that these attacks were related to the demonstrations held in Hong Kong. In November there were also incidents in which messages and images from an unknown party calling themselves the Syrian Electronic Army were displayed on a number of major sites in Japan. In these incidents, an SNS coordination service on these sites was used to redirect users to another site thought to have been prepared by the attacker, who had rewritten registration information related to the name server after gaining unauthorized access to the registry. This had an impact on many sites, including major sites in Japan and overseas that were using the corresponding service. Because there had been a number of similar incidents in which Japanese companies were affected, several organizations including the JPCERT Coordination Center issued alerts. See "1.4.1 Countermeasures Against the Alteration of Domain Name Registration Information" for more information.

### ■ Government Agency Initiatives

Government agency initiatives included passing the "Bill on Cyber Security," which had been carried over from the previous Diet session, at the Lower House plenary session in November. This is designed to strengthen systems for promoting cyber security and functionality to bolster security at government agencies, etc., such as establishing a Cyber Security Strategic Headquarters, creating security strategy plans, formulating security standards for government agencies, and investigating security incidents that occur there. It is also expected to lead to more collaborations between the state and private-sector companies, such as the promotion of security at critical infrastructure providers, and the reinforcement of public-private coordinated countermeasures.

In light of this, the 41st assembly of the Information Security Policy Council was held, and policy for initiatives related to improving the functions of systems for promoting cyber security in Japan was decided on*14. Other specific initiatives included the establishment of the "Information Security Social Promotion Association" in November. This is aimed at improving the standards of information security in Japan by enhancing the interest, understanding, and response capabilities of the nation as a whole with regard to information security. Also in November, regarding the so-called Japanese version of the NCFTA*15 discussed at the National Police Agency's General Security Countermeasures Conference, the "Japan Cybercrime Control Center (JC3)" commenced operation. Its participants include private-sector companies, academic research institutions, and investigative organizations. JC3 conducts information sharing and analysis, as well as research and development into countermeasures, in relation to cyberspace threats that participant organizations face. It also provides training, and carries out activities to promote a safe and secure cyberspace through initiatives and collaboration with overseas institutions such as U.S. NCFTA*16.

### ■ Website Alteration Techniques

In October, a website operated by a newspaper publisher in Japan was compromised and exploited as a phishing site. Due to this incident, the corresponding site was shut down and an investigation carried out, but service resumed over a month later in December after the investigation was completed and the security of the site was verified. In December, there was an incident of unauthorized access at ICANN (Internet Corporation for Assigned Names and Numbers), which manages and coordinates various Internet resources such as domains and IP addresses. After it was confirmed that a number of systems had been accessed, including the Centralized Zone Data System (czds.icann.org), it was announced that they had taken the step of disabling passwords. In this incident, the information used included passwords that had leaked through a phishing email attack in November in which the attacker posed as an internal staff member. Similarly, unauthorized access was made to the website of Internet Systems Consortium (ISC), which develops the BIND DNS server. This led to alterations that redirected users to a malware distribution site. The alterations made in this incident exploited a vulnerability in WordPress.

*14 National Information Security Center, "41st Assembly (held on a rotating basis) (November 25, 2014)" (http://www.nisc.go.jp/conference/seisaku/index.html#seisaku41) (in Japanese).

*15 Because it was specified in the cyber security strategy decided on by the Information Security Policy Council in 2013 that establishment of a Japanese version of NCFTA should be looked into, this matter was examined at the National Police Agency's General Security Countermeasures Conference (http://www.npa.go.jp/cyber/csmeeting/index.html) (in Japanese).

*16 NCFTA (National Cyber-Forensics & Training Alliance) (http://www.ncfta.net/Index.aspx) is a U.S. nonprofit organization with members comprised of law enforcement agencies such as the FBI, private-sector companies, and academic institutions. It gathers and analyzes information related to cybercrime, and conducts training for the staff of investigative organizations.

## November Incidents

**O** **5th:** Alerts were issued by a number of organizations including the JPCERT Coordination Center due to multiple domain name hijacking incidents, in which the registration information of .com domain names used by organizations in Japan was illegally altered and name server information prepared by the attacker added.
"JPCERT/CC Alert 2014-11-05 Alert on domain name hijacking by altering registration information" (http://www.jpcert.or.jp/english/at/2014/at140044.html).

**O** **6th:** The Bill on Cyber Security was passed at the Lower House plenary session.
"Bill on Cyber Security" (http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g18601035.htm) (in Japanese).

**S** **7th:** The FBI announced they had uncovered the Tor-based Silk Road 2.0 crime site that dealt in illicit drugs and arrested the operator.
FBI, "Manhattan federal court to the operator of charge Silk Road 2.0 web site" (http://www.fbi.gov/newyork/press-releases/2014/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court).

**S** **7th:** The European Police Office (Europol) announced it had uncovered a number of crime sites operated on Tor in coordination with law enforcement agencies in 16 countries including the United States and European nations.
EUROPOL, "GLOBAL ACTION AGAINST DARK MARKETS ON TOR NETWORK" (https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network).

**S** **11th:** The United States Postal Service (USPS) announced it had been accessed by an unknown party without authorization, and the personal information of over 800,000 employees may have leaked.
"Postal Service Statement on Cyber Intrusion Incident" (http://about.usps.com/news/fact-sheets/scenario/media-statement-final.pdf).

**V** **12th:** Microsoft published their Security Bulletin Summary for November 2014, and released a total of fourteen updates, including four critical updates such as MS14-064 and MS14-065, as well as eight important updates.
"Microsoft Security Bulletin Summary for November 2014" (https://technet.microsoft.com/library/security/ms14-nov).

**V** **12th:** 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/apsb14-24.html).

**V** **13th:** A vulnerability in JustSystems Corporation's Ichitaro that could allow arbitrary code executions was discovered and fixed.
JVN, "JVN#16318793 Ichitaro series vulnerable to arbitrary code execution Critical" (https://jvn.jp/en/jp/JVN16318793/).

**O** **13th:** The JC3: Japan Cybercrime Control Center was launched and began operations. This initiative is aimed at investigating cybercrime and reducing or neutralizing its threat through information sharing between industrial, government, and academic organizations and collaboration with overseas institutions, to deal with threats in cyberspace.
"Establishment of 'Japan Cybercrime Control Center,' a New Organization for Fighting Cybercrime" (https://www.jc3.or.jp/media/pdf/pressreleaseEnglish.pdf).

**O** **17th:** The inaugural meeting of the Information Security Social Promotion Association was held. The aim of this association is to build a safe and secure society through the construction of an information distribution network by national and regional organizations in industry, government and academia, allowing them to collaborate and coordinate.
National Information Security Center (NISC), "Regarding the Inaugural Meeting of the Information Security Social Promotion Association (provisional name)" (http://www.nisc.go.jp/press/pdf/syakaisuishinkyougikai20141113.pdf) (in Japanese).

**S** **19th:** The Tokyo Metropolitan and 19 prefectural police departments established a joint investigation headquarters and carried out a simultaneous search due to the illegal operation of proxy servers using unlawfully obtained IDs and passwords. This resulted in the arrest of a number of people suspected of violating the Unauthorized Computer Access Law.

**V** **21st:** A number of vulnerabilities that could allow sites to be compromised, including XSS vulnerabilities, were discovered and fixed in the WordPress CMS application.
"WordPress 4.0.1 Security Release" (https://wordpress.org/news/2014/11/wordpress-4-0-1/).

**S** **21st:** A number of people including minors were charged with violating the Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children (display in public), or were referred to a child guidance center, for proliferating child pornography images posted to Twitter by retweeting them.

**S** **24th:** An incident occurred in which a movie company in the U.S. was compromised by an unknown party, leading to their entire system being shut down.

**V** **26th:** 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/apsb14-26.html).

**S** **27th:** A U.S. SNS coordination service was targeted in a domain hijacking caused by a registry attack, leading to incidents in which certain messages and images were displayed on a large number of sites that used this service, including major domestic and international sites.
See the following Gigya blog post for more details. "Regarding Today's Service Attack" (http://blog.gigya.com/regarding-todays-service-attack/).

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

*Dates are in Japan Standard Time

The website of a publisher in Japan was also compromised, causing visitors to be redirected to another website. In this incident, phishing emails were used to direct recipients to a login form misrepresented as being for the purpose of confirming member details, thus illegally acquiring information such as IDs and passwords. The compromise was caused due to the theft of an ID with cloud service administrator privileges.

### ■ Attacks Targeting the Internal Information of Corporations

During the current survey period, leaks of internal information through malware infections in corporate business systems continued to be discovered. In October, malware infections were uncovered at a number of retailers. It was announced that one of these was affected by the Backoff malware that targets POS systems, which has been used in multiple information leaks since last year*17. US-CERT issued an alert regarding this malware in August*18, but infections have continued to occur since then, indicating that it is still very active, and ongoing caution is required.

In November there was a large-scale attack on a major movie company in the U.S. In this incident, malware infections on internal PCs led to the leak of a large amount of internal data, such as unreleased movie data, passport information for movie-related persons, email data of employees, and other personal information. The fallout from this incident continued for some time after, including threats demanding that a certain movie stay unreleased, and the release of data leaked by an unknown party multiple times. Because the malware used included a function that disabled the specific security software used by the affected company, as well as a function that destroys the data on PCs, it is thought these attacks targeted the company in question and were executed after careful preparation. A number of security companies have identified that this malware was similar to the one used in mass simultaneous malware infections that occurred at a number of broadcasting stations and financial institutions in South Korea in 2013*19*20.

In December, a power company in South Korea was attacked via emails with malware attached, leading to the leak of internal information. In this incident, the culprit demanded the shutdown of nuclear power stations as well as financial compensation, and released nuclear reactor plans and employee personal information on the Internet over a number of times.

### ■ Other

In the United States, the FBI announced they had shut down the Silk Road 2.0 crime site that dealt in illicit drugs and arrested its operator. In relation to this, the European Police Office (Europol) carried out a large-scale crackdown on crime sites operated on Tor in coordination with law enforcement agencies in 16 countries including the United States and European nations. In this operation, over 400 .onion domains that used Tor were seized. There were a large number of arrests, and Bitcoin currency, cash, a variety of drugs, and precious metals such as gold were confiscated.

In November, the Metropolitan and 19 other prefectural police departments established a joint investigation headquarters and carried out a nationwide simultaneous search due to the illegal operation of proxy servers using unlawfully obtained IDs and passwords. This resulted in the arrest of a number of people suspected of violating the Unauthorized Computer Access Law. In this incident, a number of people were also arrested on suspicion of copyright infringement (infringement of reproduction rights or business use of pirated copies) because pirated software was used on the servers operated*21. Regarding the stolen IDs and passwords, it is thought that a known vulnerability in certain wireless LAN routers was exploited, and these details used to gain unauthorized access and conduct phishing attacks on major banks.

Also in November, the malware known as Regin received widespread attention. It is said a provider in Belgium was infected with this malware, which is designed to conceal itself within a network it has compromised and monitor communications. In

*17 International Dairy Queen, Inc. “Data Security Incident” (http://www.dairyqueen.com/datasecurityincident/).

*18 US-CERT, “Alert (TA14-212A) Backoff Point-of-Sale Malware” (https://www.us-cert.gov/ncas/alerts/TA14-212A).

*19 See “1.4.1 The 3.20 Cyber Attack in South Korea” in IIR Vol.19 (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol19_EN.pdf) for more information about this incident.

*20 See the following Trend Micro security intelligence blog post for more information: “An Analysis of the ‘Destructive’ Malware Behind FBI Warnings” (http://blog.trendmicro.com/trendlabs-security-intelligence/an-analysis-of-the-destructive-malware-behind-fbi-warnings/).

*21 Association of Copyright for Computer Software “Nationwide Simultaneous Crackdown on Operators of Malicious Proxy Servers” (http://www2.accsjp.or.jp/criminal/2014/post.php) (in Japanese).

## December Incidents

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

S **6th:** An incident occurred in which the website of a publisher was compromised by an unknown party, and altered to redirect visitors to another website.

O **8th:** The National Information Security Center held an intersectoral exercise for critical infrastructure.
"Summary of Intersectoral Exercise for Critical Infrastructure [2014 Annual Intersectoral Exercise]"
(http://www.nisc.go.jp/active/infra/pdf/bunya_enshu2014gaiyou.pdf) (in Japanese).

V **9th:** A vulnerability that could cause abnormal operations on a server or stop a service was discovered and fixed in a number of DNS software implementations such as BIND.
CERT/CC, "Vulnerability Note VU#264212 Recursive DNS resolver implementations may follow referrals infinitely"
(https://www.kb.cert.org/vuls/id/264212).

V **10th:** Microsoft published their Security Bulletin Summary for December 2014, and released a total of seven updates, including three critical updates such as MS14-080 and MS14-081, as well as four important updates.
"Microsoft Security Bulletin Summary for December 2014" (https://technet.microsoft.com/library/security/ms14-dec).

V **10th:** 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/apsb14-27.html).

V **10th:** A number of vulnerabilities in Adobe Reader and Acrobat that could allow arbitrary code execution were discovered and fixed.
"APSB14-28: Security updates available for Adobe Reader and Acrobat" (http://helpx.adobe.com/security/products/reader/apsb14-28.html).

S **15th:** Korea Hydro & Nuclear Power was attacked using email with malware attached, leading to the leak of nuclear reactor plans and manuals, as well as the personal information of employees.

S **17th:** ICANN announced that a number of systems had been accessed without authorization, and some user information had leaked.
See the following ICANN announcement for more details: "ICANN Targeted in Spear Phishing Attack | Enhanced Security Measures Implemented" (https://www.icann.org/news/announcement-2-2014-12-16-en).

O **17th:** The Federal Office for Information Security (BSI) of the German Federal Ministry of the Interior published its 2014 IT security white paper.
The white paper states that an incident occurred in which a steel mill was attacked, causing damage to the facilities. See "3.3.1 APT attack on industrial installations in Germany" in "The State of IT Security in Germany 2014"
(https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014_pdf.pdf?__blob=publicationFile) for more information about this incident.

O **18th:** CODE BLUE, an international information security conference originating in Japan, was held over two days.
See the following official site for CODE BLUE for more information (http://www.codeblue.jp/2014/en/).

O **19th:** The JPCERT Coordination Center issued an alert due to an increase in scans to TCP port 8080 from around December 5. This was scanning behavior targeting the NAS products provided by QNAP Systems, Inc.
"JPCERT/CC Alert 2014-12-19 Alert regarding increase in scans to TCP port 8080" (http://www.jpcert.or.jp/english/at/2014/at140055.html).

V **20th:** A number of vulnerabilities in ntpd that could allow arbitrary code execution with ntpd privileges by sending specially-crafted packets were discovered and fixed.
CERT/CC, "Vulnerability Note VU#852879 NTP Project Network Time Protocol daemon (ntpd) contains multiple vulnerabilities (Updated)"
(http://www.kb.cert.org/vuls/id/852879).

O **22nd:** The Ministry of Internal Affairs and Communications made revisions to their "Guidelines for Unlocking Sim Lock," which is one of the initiatives aimed at lowering the cost of mobile services and encouraging more diversity. In these guidelines it is stated that all devices sold by carriers should support the unlocking of SIM cards in principle.
"Revisions to 'Guidelines for Unlocking SIM Lock'" (http://www.soumu.go.jp/menu_news/s-news/01kiban03_02000275.html) (in Japanese).

S **23rd:** An incident occurred in which the website of the Internet Systems Consortium (ISC) was accessed without authorization, and altered to redirect visitors to a malware distribution site.
See the following blog post from U.S. security firm Cyphort that discovered the issue for more information. "Internet Systems Consortium's ISC.org infected" (http://www.cyphort.com/isc-org-infected/).

V **28th:** At a security conference held in Germany, it was announced that the SS7 telecommunication standard used in public telephone networks has a vulnerability that could allow wiretapping.
See the following announcement for more information about this vulnerability. Laurent Ghigonis, Alexandre De Oliveira, "SS7map : mapping vulnerability of the international mobile roaming infrastructure"
(http://media.ccc.de/browse/congress/2014/31c3_-_6531_-_en_-_saal_6_-_201412272300_-_ss7map_mapping_vulnerability_of_the_international_mobile_roaming_infrastructure_-_laurent_ghigonis_-_alexandre_de_oliveira.html#video).

V **29th:** Google announced it had found a vulnerability with no fix available in Microsoft's Windows 8.1 Update that could lead to the elevation of privileges.
This information was disclosed at google-security-research (https://code.google.com/p/google-security-research/).

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

*Dates are in Japan Standard Time

addition to standard RAT functions such as password theft and network traffic monitoring, special functions such as a feature for monitoring mobile phone base stations have also been confirmed*22.

In December, the Federal Office for Information Security (BSI) of the German Federal Ministry of the Interior published an IT security white paper, which revealed that attacks on a steel mill had caused damage to production facilities due to their shutdown.

A number of large-scale DDoS attacks occurred during this period. In December, an unknown entity calling themselves the Lizard Squad attacked a number of online game services such as PSN and Xbox Live, as well as Tor. The attackers subsequently provided the attack platform used in this series of attacks as a DDoS attack tool, and this was actually used in DDoS attacks on a number of sites. In January a number of people thought to be members were arrested, but as attacks continue to be made by remaining members afterwards, ongoing vigilance is necessary.

## 1.3 Incident Survey

### 1.3.1 DDoS Attacks

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

**■ Direct Observations**

Figure 2 shows the circumstances of DDoS attacks handled by the IIJ DDoS Protection Service between October 1 and December 31, 2014.

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*23, attacks on servers*24, and compound attacks (several types of attacks on a single target conducted at the same time).

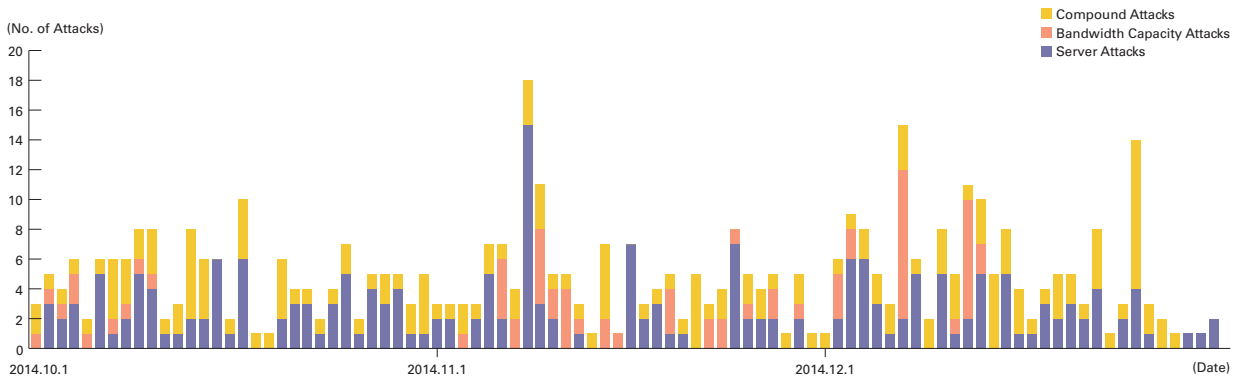



**Figure 2: Trends in DDoS Attacks**

*22 See the following Symantec Security Response Blog post for more information about this malware. "Regin: Top-tier espionage tool enables stealthy surveillance" (http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance)

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

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

During the three months under study, IIJ dealt with 381 DDoS attacks. This averages to 4.14 attacks per day, indicating an increase in the average daily number of attacks compared to our prior report. Server attacks accounted for 54.6% of all incidents, while compound attacks accounted for 26.9%, and bandwidth capacity attacks 18.6%. The largest attack observed during the period under study was classified as a compound attack, and resulted in 3.1 Gbps of bandwidth using up to 432,000 pps packets.

Of all attacks, 90.8% ended within 30 minutes of commencement, 9.2% lasted between 30 minutes and 24 hours, and none lasted over 24 hours. The longest sustained attack was a compound attack that lasted for six hours and 28 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*25 and botnet*26 usage as the method for conducting DDoS attacks.

### ■ Backscatter Observations

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

For the backscatter observed between October 1 and December 31, 2014, Figure 3 shows the sender's IP addresses classified by country, and Figure 4 shows trends in packet numbers by port.

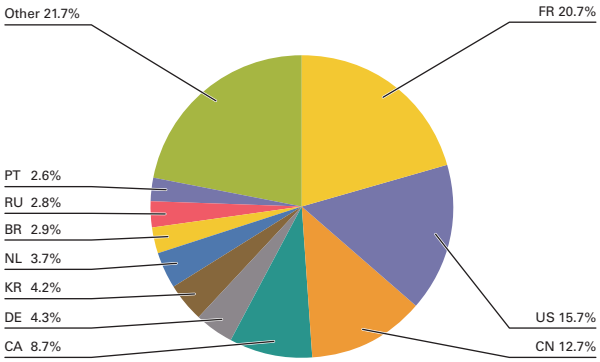



**Figure 3: DDoS Attack Targets by Country According to Backscatter Observations**

The port most commonly targeted by the DDoS attacks observed was the 80/TCP port used for Web services, accounting for 35.1% of the total during the target period. This was followed by 53/UDP used for DNS at 22.8%, so the top two ports accounted for 57.9% of the total. Attacks were also observed on 6667/TCP used for IRC (Internet Relay Chat) and 443/TCP used for HTTPS, as well as the typically unused 0/TCP, 34000/TCP, and 25565/TCP.

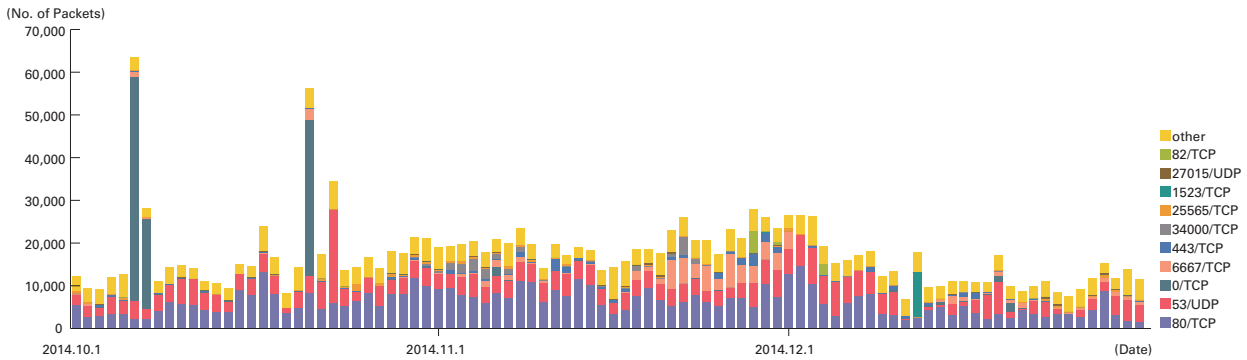



**Figure 4: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)**

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

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

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

*28 The mechanism and limitations of this observation method, as well as some of the results of IIJ's observations, are presented in Vol.8 of this report (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 53/UDP backscatter that has been prevalent in observations since February 2014 remains the second highest in number of packets observed by port in this survey. However, the daily average has increased from approximately 3,100 packets to approximately 3,900 packets.

Looking at the origin of backscatter thought to indicate IP addresses targeted by DDoS by country in Figure 3, France accounted for the largest ratio at 20.7%. The United States and China followed at 15.7% and 12.7%, respectively.

Looking at particularly large numbers of backscatter packets observed by targeted port, there were attacks on the Web servers (80/TCP) of a news site in Portugal between October 16 and November 23, and on a game-related site in Germany between November 17 and November 20. Attacks were also observed on a Spanish news site between October 14 and October 18. Between October 6 and October 7, as well as on October 21, many attacks were observed on 0/TCP. Backscatter from a wide range of IP addresses was received on many honeypots, and the purpose of the attacks is not known. Other observations included ongoing attacks from October 23 on 80/TCP, 6667/TCP, and 34000/TCP targeting IRC servers in France.

Notable DDoS attacks during the current survey period that were detected via IIJ's observations of backscatter included attacks on the site of a municipal authority in the U.S. city of Phoenix, Arizona on October 22. Attacks were also detected on Ukraine's election commission on October 26, and on the site for a political party in France on November 29.

### 1.3.2 Malware Activities

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

#### ■ Status of Random Communications

Figure 5 shows the distribution of sender's IP addresses by country for communications coming into the honeypots between October 1 and December 31, 2014. 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

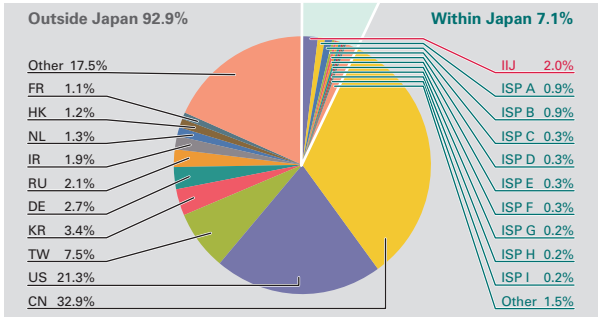



**Figure 5: Sender Distribution (by Country, Entire Period under Study)**

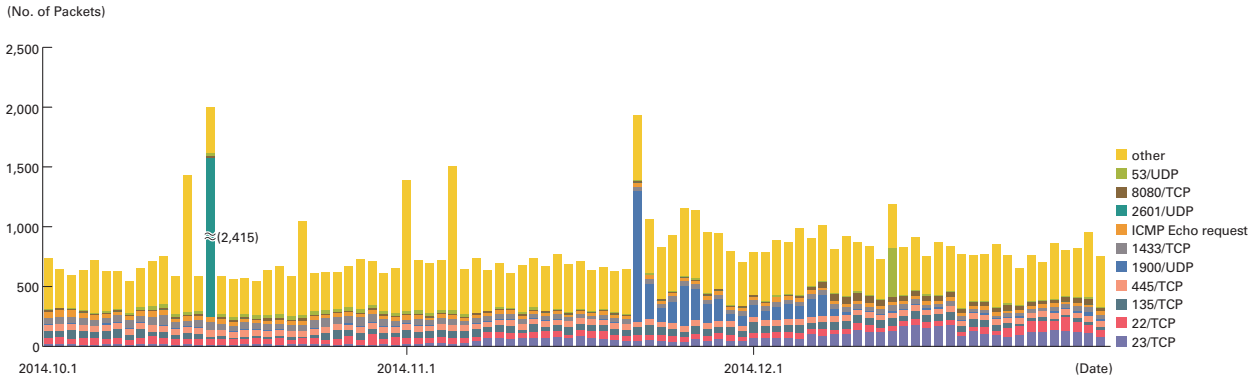



**Figure 6: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)**

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

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

the 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, 53/UDP used for DNS, 23/TCP used for Telnet, and 8080/TCP used for HTTP proxies. During the current period, there was an increase in 1900/UDP communications used in UPnP's SSDP between late November and early December. These packets involved repeated m-search requests within a short time period. It is thought these were attempted SSDP reflection attacks (a type of DDoS attack) with the sender's IP addresses spoofed, which means these source addresses in fact indicated the targets of the attacks*31. The National Police Agency issued an alert regarding these incidents in October*32.

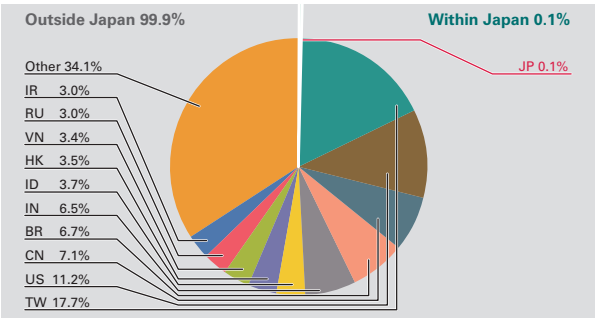



**Figure 7: Distribution of the Number of Malware Specimens Acquired**

From November there was an increase in communications targeting telnet (23/TCP). Upon investigation, we learned that this was mainly received from IP addresses allocated to China and Japan. From December 5, there was an increase in communications targeting 8080/TCP. We believe these were attacks on the Shellshock vulnerability in QNAP

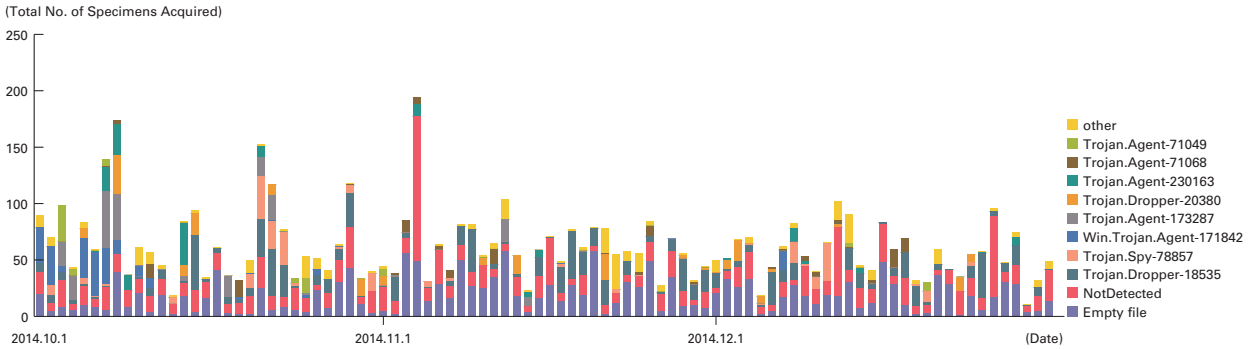



**Figure 8: Trends in the Total Number of Malware Specimens Acquired (Excluding Conficker)**

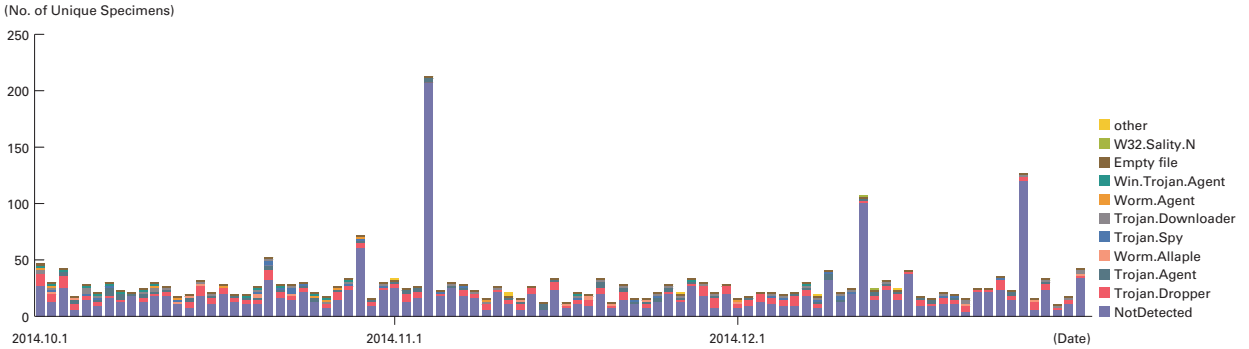



**Figure 9: Trends in the Number of Unique Specimens (Excluding Conficker)**

*31 MITF honeypots have SSDP disabled, so do not assist the attacks.

*32 "Alert regarding SSDP reflector attacks using UPnP compatible network devices as stepping stones" (http://www.npa.go.jp/cyberpolice/detect/pdf/20141017.pdf) (in Japanese).

brand NAS products*33, etc. On December 13, there was a large volume of communications targeting 53/UDP. Most of these packets were due to incoming DNS amp attack attempts*34. Because the source was spoofed to an IP address assigned to a telecommunications company in Germany, it is possible that this IP address was the target. The queries contained A record resolution requests for an existing domain, but approximately 250 A records were set to that FQDN. This resulted in a DNS amp attack, as using a spoofed source to perform name resolution for a domain set with a large number of A records causes responses to be amplified. On October 15, communications targeting 2601/UDP were made to the IP address of a specific honeypot from an IP address allocated to China. Upon investigating these communications, we found that random data with a length between 50 bytes and around 800 bytes had been sent repeatedly within a short space of time, but the purpose is not known.

### ■ Malware Network Activity

Figure 7 shows the distribution of the specimen*35 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, while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*36. Specimens are also identified using anti-virus software, and a breakdown of the top 10 variants is displayed color coded by malware name. As with our previous report, for Figure 8 and Figure 9 we have detected Conficker using multiple anti-virus software packages, and removed any Conficker results when totaling data.

On average, 63 specimens were acquired per day during the period under study, representing 17 different malware. After investigating the undetected specimens more closely, they included worms observed from IP addresses allocated to countries such as India, the United States, and Taiwan. Additionally, about 54% 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 sites that newly-infected PCs access to download malware. Under the MITF's independent analysis, during the current period under observation 93.4% of malware specimens acquired were worms, and 6.6% were downloaders. In addition, the MITF confirmed the presence of 106 botnet C&C servers*37 and 7 malware distribution sites. The number of botnet C&C servers rose dramatically, but this was due to the appearance of a specimen that used a DGA (Domain Generation Algorithm) during the current survey period.

### ■ Conficker Activity

Including Conficker, an average of 16,343 specimens were acquired per day during the period covered by this report, representing 557 different malware. While figures rise and fall over short periods, Conficker accounts for 99.6% 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. The total number of specimens acquired during the period covered by this report dropped considerably, at approximately 36% lower than the previous survey period. Unique specimens were also down by about 17%. According to the observations of the Conficker Working Group*38, as of January 13, 2015, a total of 890,845 unique IP addresses are infected*39. This indicates a drop to about 28% of the 3.2 million PCs observed in November 2011, but it demonstrates that infections are still widespread.

*33 It was also reported in JPCERT/CC observations that scanning and attacks increased on the same day. "Alert regarding increase in scans to TCP port 8080" (http://www.jpcert.or.jp/english/at/2014/at140055.html).

*34 The MITF honeypots do not query authoritative servers or cache servers when they receive DNS query packets, so they provide no aid to attacks.

*35 This indicates the malware acquired by honeypots.

*36 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.

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

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

*39 For some reason Conficker Working Group data appears to be missing for about a month from mid-December 2014, so we have cited data for January 13, 2015 that should not be affected.

### 1.3.3 SQL Injection Attacks

Of the types of different Web server attacks, IIJ conducts ongoing surveys related to SQL injection attacks*40. 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 October 1 and December 31, 2014. Figure 11 shows trends in the numbers of attacks. These are a summary of attacks detected by signatures on the IIJ Managed IPS Service.

Japan was the source for 30.8% of attacks observed, while the United States and China accounted for 13.5% and 13.4%, respectively, with other countries following in order. There was a decrease in the number of SQL injection attacks on Web servers compared to the previous report, but this is due to a significant spike in attacks originating from China in the last survey period, so there was no change in overall detection trends.

During this period, large-scale attacks from a specific attack source in France directed at specific targets took place on October 12. Attacks on these targets were confirmed from specific attack sources in Russia on October 10 and October 16, and from specific attack sources in Indonesia on December 18. On October 6, attacks were made from a number of sources in Europe and the United States directed at specific targets. On October 7, attacks originating in the Czech Republic were made on specific targets. Attacks from a specific attack source in Japan directed at specific targets also took place on October 23. On November 24, there were attacks from a specific attack source in China directed at specific targets. These attacks are thought to have been attempts to find vulnerabilities on Web servers.

As previously shown, attacks of various types were properly detected and dealt with in the course of service. However, as these attacks are ongoing, they continue to require attention.

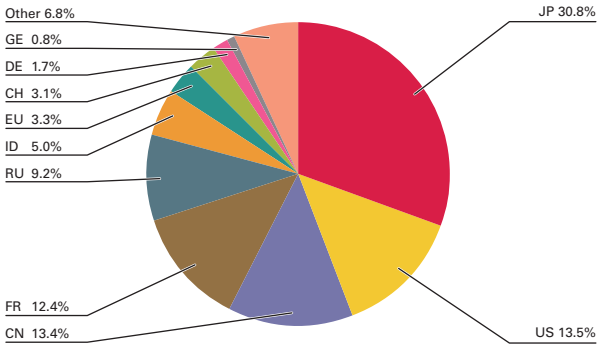



**Figure 10: Distribution of SQL Injection Attacks by Source**

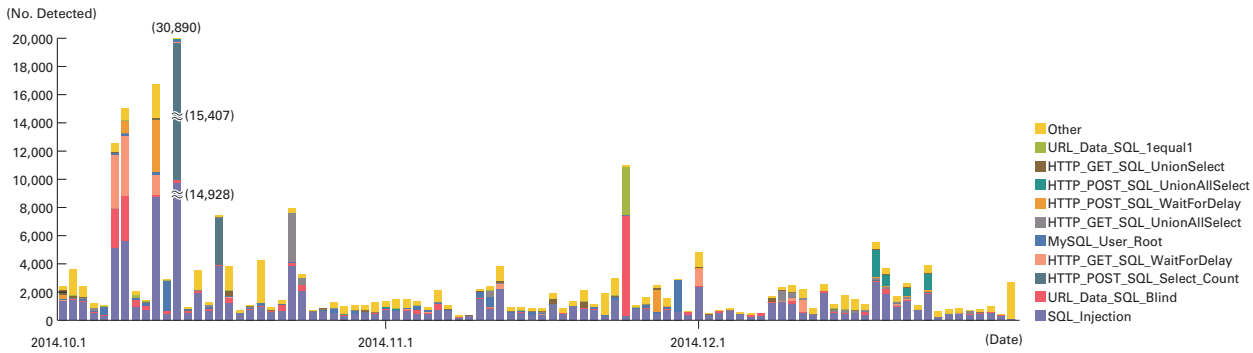



**Figure 11: Trends in SQL Injection Attacks (by Day, by Attack Type)**

*40 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)*41. 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 October and December 2014 fell to about a third of those in the period from July to September (Figure 12). In particular, there were many days in December in which no attacks were observed. Anglar continued to account for many attacks as in the previous survey, making up the majority along with Fiesta, which saw a sudden rise in this survey period. Like most other exploit kits, Fiesta is equipped with functions that exploit vulnerabilities in Internet Explorer and its plug-ins, as well as Flash, Java, and Silverlight. A recent trend in many exploit kits such as Anglar and Fiesta is that functions for exploiting a number of comparatively new Flash vulnerabilities (including CVE-2014-8439, CVE-2014-0515, and CVE-2014-0497) have been added at a rapid pace*42. Conversely, we no longer see as many functions exploiting Java vulnerabilities that were previously often targeted. We believe this is because of improvements made to Java-related security functions in popular browser environments. In 2014, a function that blocks the automatic execution of older versions of Java was added to Internet Explorer, and the automatic execution of Java was also completely blocked in Chrome and Firefox.

Most websites altered to redirect visitors were small-scale sites that are less popular, and we observed intermittently that individual sites were used as redirect sites for periods between a few days and approximately two months. With regard to trends in content, there were many sites that introduce adult-oriented video content, and websites for idol groups and design businesses among others were also altered.

Overall, it is estimated that the incidence rate for drive-by downloads is declining sharply. However, there is always the possibility of a sudden change in trends such as this depending on the intentions of attackers. 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).

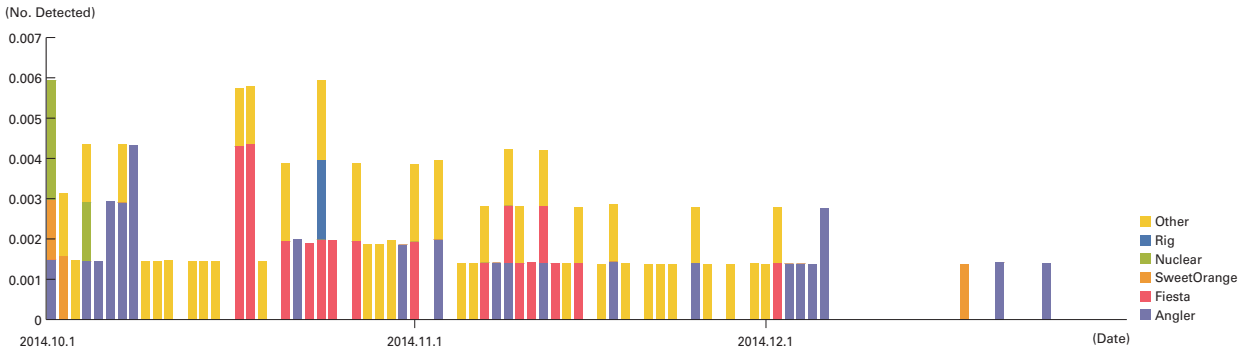



**Figure 12: Drive-By Download Frequency When Viewing Websites**

*41 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.

*42 Details of the vulnerabilities targeted by each exploit kit are summarized in the "ExploitPackTable_2014" (https://docs.google.com/spreadsheet/ccc?key=0AjvsQV3iSLa1dE9EVGhjeUhvQTNReko3c2xhTmphLUE)

## 1.4 Focused Research

Incidents occurring over the Internet change in type and scope from one minute to the next. Accordingly, IIJ works toward implementing countermeasures by continuing to perform independent surveys and analyses of prevalent incidents. Here we will present information from the surveys we have undertaken during this period, including an overview of countermeasures against the alteration of domain name registration information, and discussion of the openioc_scan plug-in used to scan for threats that lurk in the memory of a computer. We also take a look at ID management technology.

### 1.4.1 Countermeasures Against the Alteration of Domain Name Registration Information

#### ■ The Threat of Altered Domain Name Registration Information

Domain names play an important role in the Internet world. For example, when a client accesses www.example.com, it sends a query to the authoritative DNS server for the example.com zone that the server is associated with to obtain that server's IP address (Figure 13 left). This series of exchanges is called name resolution.

However, there are attacks that cause a server prepared by an attacker to be accessed instead of the legitimate server as a result of name resolution. These attacks are called domain hijackings. The attack techniques used include compromising the DNS server of the domain owner and rewriting records, making a recursive DNS server cache a malicious IP address using DNS cache poisoning, and routing specific traffic to a network other than the intended one by advertising incorrect information to BGP.

The impact of attack techniques such as these is diminishing due to countermeasures implemented by ISPs and service providers. However, a number of domain hijackings using a different attack technique occurred in September 2014 and beyond, affecting the domains of companies in Japan. This attack technique involves altering the registration information for a domain name registered to a registry so that it responds with the IP address of a server prepared by the attacker when name resolution is performed. As a result, even if the correct domain name is entered, the server prepared by the attacker is accessed, potentially exposing users to harm such as phishing attempts or malware infections. One characteristic of this technique is that servers are affected by attacks even if their security level is high, because fake information is registered on the authoritative DNS server for the top-level domain (TLD)*43 (Figure 13 right). Furthermore, because the fake information

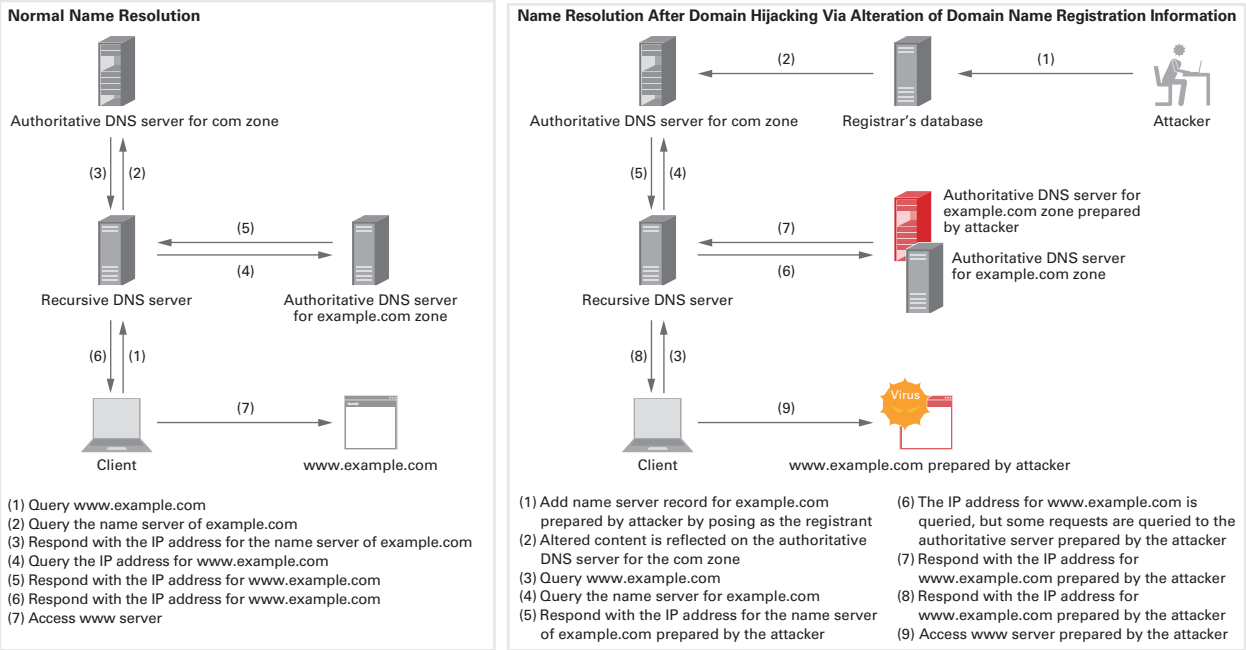



**Figure 13: Name Resolution of www.example.com (DNS protocols partially omitted)**

*43 Indicates the right-most label of domain names delimited by a dot (.), such as "jp" and "com" in "www.example.jp" and "mail.example.com," respectively.

only has to be registered to an authoritative DNS server upstream of the domain the server belongs to, when the domain hierarchy is deep, the fake information may be registered to an authoritative DNS server of a second-level domain (SLD) rather than a TLD.

In the incidents that occurred between September and October 2014, attacks that caused Web page visitors to download malware were made on ".com" domains owned by a number of companies in Japan[*44][*45]. Additionally, in November 2014 there were incidents affecting major domestic and international newspaper publishers and news sites using an SNS coordination service provided by an overseas company. In these incidents, Web page visitors were served with malicious JavaScript files that caused the crest of the Syrian Electronic Army (SEA) to be displayed.

In the incidents in November 2014, all NS records were altered to those of the attacker, forcing the malicious JavaScript to be always served. However, in the incidents affecting the domains of domestic companies between September and October, the attacker's NS records were added without deleting the legitimate NS records. For this reason, only some users were affected.

Many attacks using techniques similar to these have already occurred overseas. For example, in 2013 a large number of registries were attacked, and incidents occurred on almost a monthly basis[*46].

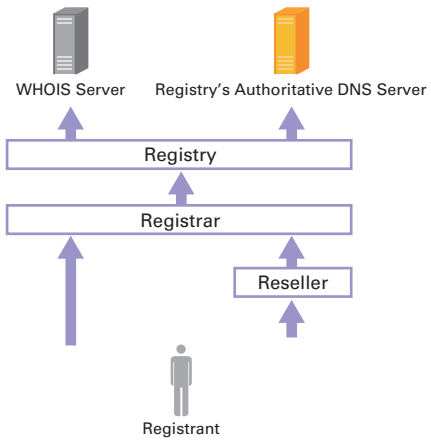
### ■ Techniques for Altering Domain Name Registration Information

Information regarding domains is registered in the databases of organizations called registries, which operate and manage TLDs. To register a domain, a domain registration application is sent to a registry using the services of an intermediary called a registrar (or a reseller of the registrar's services). Domain registration information is passed on in the order shown by the arrows in Figure 14, and registered to the registry's authoritative DNS server and WHOIS server.

Consequently, attackers alter domain name registration information by attacking any of the points below.

(1) Registrar data is altered by stealing the identity of the registrant or reseller.
(2) Registry data is altered by stealing the identity of the registrar.
(3) Data is altered using a vulnerability on the system of the registry or registrar.

Identity theft is carried out based on information gained through methods such as phishing, malware infections, or social engineering targeting the domain registrant. Leaked account information for registries or registrars and list-based attacks are also potential causes.




Registry's authoritative DNS server: database that links servers belonging to a domain and IP addresses
WHOIS server: database of information about domains and contact information of registrants

(4) Organization that manages and operates top-level domains (TLDs). Registers domain information to authoritative DNS servers and WHOIS servers.

(3) Acts as an agent for domain information registration applications to registries from registrants or resellers.

(2) Sells the services of registrars. Acts as an agent for domain information registration applications to registrars from registrants.

(1) Submits domain information registration applications to registrars or resellers.

**Figure 14: Domain Information Registration Process**

*44 Democracy in Hong Kong Under Attack | Volexity Blog (http://www.volexity.com/blog/?p=33).
*45 IIJ has not observed cases in which malware infections took place.
*46 Japan Registry Services (JPRS), "Additional Reference: Regarding domain name hijackings caused by unauthorized rewriting of registered information and their countermeasures" (http://jprs.jp/tech/security/2014-11-05-unauthorized-update-of-registration-information.pdf) (in Japanese).

The data altered is the name servers registered to the registry's WHOIS server and the NS records and glue records registered to the authoritative DNS server.

### Countermeasures

Here we explain countermeasures against the alteration of domain name registration information.

#### Registries/Registrars/Resellers

The most fundamental security measure is to ensure that fixes and patches for vulnerabilities in OSes, Web applications, and APIs are applied. Measures such as applying patches and installing antivirus software on clients within the organization must also be taken.

Next you should contemplate improving functions for authenticating user accounts to protect against identity theft. It is likely that many systems perform authentication using passwords, so it is necessary to set complicated passwords and prevent reuse of the same password. If possible, also consider implementing two-step authentication or authentication based on client certificates.

Additionally, look into implementing functions for monitoring and sending notification of user activity. It is possible to detect actions not intended by the user by sending notification of account logins and changes to registration information. Furthermore, if there is a history of this, users can confirm when unauthorized access began themselves.

To protect against actual attacks, it is necessary to implement systems for detecting and dealing with attacks. Attacks are detected based on security devices, system load, or logs, and blocked using a firewall, etc., as appropriate.

Finally, consider providing a Registry Lock service. This is a function that restricts changes to a registration information at a registry, making it possible to prevent unintended changes to information because additional authentication is required of the registrant when changing registration information.

There have also been cases in which services for resetting email addresses or passwords by fax have been exploited at overseas registrars. If you provide a similar service, it would be advisable to review the need for this service and the process for identity confirmation.

#### Registrants

It is important to select a registry/registrar that implements measures such as those detailed above. Proactively use features provided by registrars such as improved authentication, notification functions, and Registry Lock. Also apply OS patches and use the latest versions of software. Additionally, install antivirus software. You should also never reuse the same passwords for registrar accounts.

When using a notification function, configure settings so that notification emails are not detected as spam. When doing this, the contact email address should be on a domain other than one you have registered. This enables you to contact the registrar, even if domain name registration information is altered. If there is an option for not displaying registrant information in the public WHOIS information, consider enabling this.

Furthermore, you may be able to detect the alteration of registration information earlier by periodically confirming that information registered to the WHOIS server and registry's authoritative DNS server has not been altered. Check the name server on the WHOIS server, and the domain's NS records and glue records on the registry's authoritative DNS server.

However, because there is no standardized tool for monitoring this information, it is necessary to create your own. We have confirmed a number of monitoring tools released on voluntary basis, but it is necessary to confirm their behavior sufficiently before using them, since some only monitor specific records or do not send queries directly to a registrar's authoritative DNS server.

Furthermore, when performing monitoring, do not send more queries than necessary to a registry's authoritative DNS server or WHOIS server. If you send excessive queries, they may be detected as an attack on the registry, causing them to be restricted or blocked.

### General Users

It is almost impossible for general users to determine whether or not domain name registration information has been altered. Consequently, apply OS patches, use the latest versions of software, and install antivirus software to prevent vulnerabilities being exploited when you access a server prepared by an attacker.

Additionally, because it is not possible to steal the SSL/TLS private keys of a server by altering domain name registration information, attackers cannot provide services that carry out SSL/TLS encryption. For this reason, when you access a service normally provided via HTTPS using HTTP, or encounter SSL/TLS errors, it is possible that domain name registration informationhas been altered, so it would be advisable to stop using that service.

### Summary

At this point in time the most effective countermeasure is Registry Lock, but some registries do not provide this function. Furthermore, by implementing the countermeasures detailed here regardless of whether Registry Lock is used, you can prevent the alteration of domain name registration information, or detect it at an early stage, just in case Registry Lock is compromised.

The larger the number of users that a domain provides services to, the greater the impact, so take this opportunity to implement countermeasures now.

## 1.4.2 The openioc_scan Plug-in That Scans for Threats Lurking in Device Memory

An IOC (indicator of compromise) is an artifact left on a network or computer that indicates a threat of malware infection or intrusion. By defining IOCs based on the results of malware or forensic analysis, it is possible to detect the same threat swiftly the next time it occurs. In this section, we introduce a tool IIJ has implemented that scans for IOCs in computer memory, and discuss a study regarding using it with generic IOCs.

### Background to Implementation

The term IOC does not refer to a specific format or implementation. At a site called IOC Bucket*47, IOCs are shared in a number of formats. Figure 15 shows the number and ratio of IOC formats shared on this site (as of January 8, 2015).

From this figure, we can see that OpenIOC*48 accounts for over three quarters of all formats, making it the most prevalent major format. As mentioned in a previous IIJ SECT blog article*49, there are free tools such as IOC Finder and Redline that perform scans based on OpenIOC definitions. IOC Finder is a tool for scanning systems as they are running, enabling an effective live response. Meanwhile, Redline scans saved memory images offline. In the latter case, being offline makes it possible to disable the concealment of information by malware, and define the characteristics of strings in memory as well as code after unpacking, so you can make definitions based on malware functions.

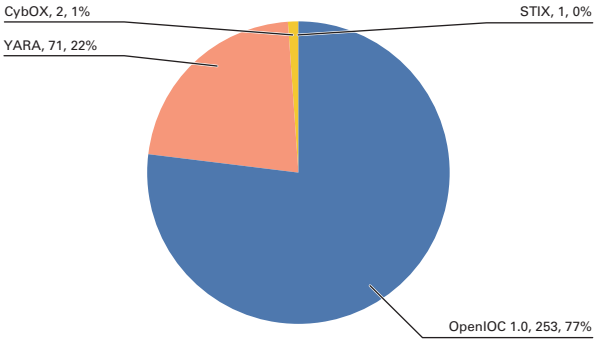



**Figure 15: Number and Ratio of IOC Formats Shared on IOC Bucket**

Up until now, IIJ has conducted evaluations for the early detection of malware using OpenIOC and Redline*50. However, Redline is a closed source tool, so there was a problem in that we could not extend its functions or fix bugs ourselves. Consequently, we implemented a plug-in for the open source Volatility Framework*51 tool, called openioc_scan*52.

*47 An IOC sharing site run by volunteers. As of January 8, 2015, 327 IOCs have been shared (https://www.iocbucket.com/search).

*48 A standard promoted by Mandiant. IOCs are written in XML format (http://openioc.org/).

*49 This article describes examples utilizing the OpenIOC free tool. "Defining and detecting traces of the presence of threats using OpenIOC" (https://sect.iij.ad.jp/d/2012/02/278431.html) (in Japanese).

*50 At the SANS DFIR Summit 2013 the year before last, we gave a presentation regarding techniques for defining and detecting volatile IOCs (https://digital-forensics.sans.org/summit-archives/DFIR_Summit/Volatile-IOCs-for-Fast-Incident-Response-Haruyama.pdf).

*51 An open source memory forensic tool for which a variety of plug-ins are made available by volunteers (https://github.com/volatilityfoundation/volatility).

*52 The latest version is available from the following link (http://takahiroharuyama.github.io/blog/2014/08/15/fast-malware-triage-using-openioc-scan-volatility-plugin/).

### openioc_scan

Here we will describe how openioc_scan is used. Analysis using openioc_scan can only be performed on Windows OSes from Vista onward*53, as Linux and Mac OS X are not currently supported. Additionally, the three Python packages lxml*54, ioc_writer*55, and colorama*56 are required to execute it. IOCs must also be defined in advance. To support regular expressions and the parameters described below, openioc_scan uses the OpenIOC 1.1 format. Currently, the only free tool capable of OpenIOC 1.1 definitions is PyIOCe*57, which we will use to define IOCs in the following description.

Figure 16 shows part of the PyIOCe screen. Users define the terms (items) for volatility on this screen. In the figure, the two terms ProcessItem/ParentProcessName and ProcessItem/name are combined using AND/OR logic and defined. In addition to being able to specify NOT (negation) as shown in the figure, it is also possible to differentiate between upper-case and lower-case characters, and specify matching*58.

Once IOCs are defined, the folder where these definition files are located is specified using the ioc_dir option, and openioc_scan is executed as shown in Figure 17. In principle, if combining the evaluation results for each term using AND/OR results in a true match, the term that is a true match for that IOC is displayed in a different color. In the figure, we can see that svchost.exe with the process ID 2204 is the process that matched the criteria. Incidentally, unlike Redline, Volatility Framework does not cache the analysis results for memory images. However, openioc_scan caches the information required for the evaluation of each term on a case-by-case basis, so it is possible to perform processing at high speed when evaluating the same term a second and subsequent time*59.

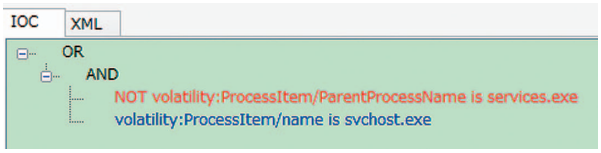



**Figure 16: Example of IOC Definition Using PyIOCe**

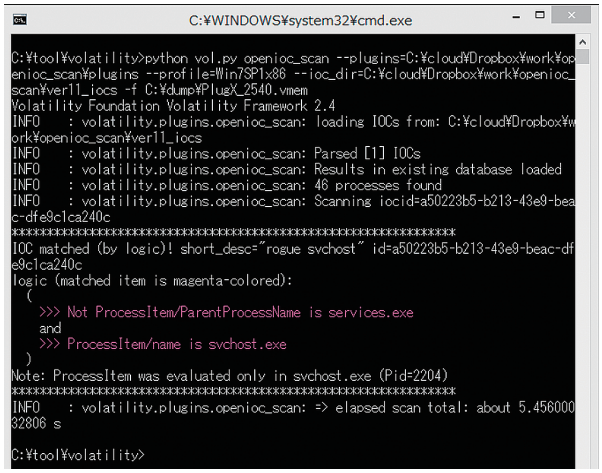



**Figure 17: openioc_scan Execution**

Table 1 shows a list of terms that openioc_scan supports. Regarding ProcessItem and DriverItem, the processes and drivers to be scanned are evaluated individually to check if they are a true or false match with IOC definitions. For example, the IOCs in the previous example are evaluated within a single process. It is also possible to make definitions that combine terms from different categories. However, this may dramatically decrease performance depending on the combination*60, so for definitions it would be better to define terms simply in a single category whenever possible.

Previously, it was stated that in principle, if combining the evaluation results for each term using AND/OR results in a true match, the term that is a true match for that IOC is displayed in a different color. In fact, there is a method for displaying IOCs even when the final result of AND/OR for a term is not true.

OpenIOC 1.1 uses the concept of parameters to enable metadata to be defined for each term. In openioc_scan, scoring-based evaluation is supported using these

*53 It is actually also possible to scan memory images of XP and 2003 for items other than communications information, but this is not supported as sufficient testing has not been carried out.
*54 A package for parsing XML (https://pypi.python.org/pypi/lxml/3.2.1).
*55 A package for parsing OpenIOC 1.1 items (https://github.com/mandiant/ioc_writer)
*56 A package for changing the color of the text output in the console (https://pypi.python.org/pypi/colorama).
*57 An open source tool by Sean Gillespie (https://github.com/yahoo/PyIOCe).
*58 It is possible to specify is/contains/matches/starts-with/ends-with/greater-than/less-than based on factors such as whether the object to be scanned is a character string or numerical value. Regular expressions are specified for matches.
*59 Only information related to terms that take time are cached, such as the extraction of character strings. If the type of term is the same, it is processed at high speed even if the values are changed.
*60 For example, ProcessItem and DriverItem often involve iterative processing, so when making definitions that combine terms belonging to each of these categories, execution tends to take longer.

parameters. For example, when evaluating the IOC in the previous example, even if only one of the terms is true, when a score defined as a parameter exceeds the threshold, the fact there was a match to the IOC based on the score is shown. Specifically, when a score set to the parameters exceeds an integer value total of 100, the corresponding IOC is displayed as shown in Figure 18. In openioc_scan, parameters such as detail and note are also supported*61.

### ■ Study Regarding Generic IOCs

Generally, IOCs are used to detect known threats. The main reason for this is that the majority of previous IOCs are defined with information such as the MD5 hash signature of malware or the URL of a C&C server, which would be hard to reuse to detect unknown threats. Consequently, IIJ carried out a study of generic IOCs for openioc_scan that are independent of specific malware or incidents.

Table 2 summarizes the evaluation results. With generic definitions you cannot completely avoid false positives, so it is not possible for just anyone to detect unknown threats using the IOCs studied here. However, from the perspective of assigning

**Table 1: Terms Supported by openioc_scan**

| Term Category | Term Type |
|---|---|
| ProcessItem | Process name, path name, argument, parent process name, DLL path name, presence of DKOM*62, presence of code injection, used API name, character string, handle name, network connection information, hooked API name, effective privilege type |
| RegistryItem | History of executable files accessed by OS (ShimCache*63) |
| ServiceItem | Service name, descriptive name, command line |
| DriverItem | Driver name, used API name, character string, IRP function table*64 hooks, callback function type, timer function presence |
| HookItem | Hooked SSDT entries*65 |
| FileItem | Metadata type of file based on MFT entries*66 |

```
**********************************************************************
IOC matched (by score)! short_desc="rogue svchost" id=a50223b5-b21
logic (matched item is magenta-colored):
  (
    Not ProcessItem/ParentProcessName is services.exe
    and
    >>> ProcessItem/name is svchost.exe (score=100;)
  )
Note: ProcessItem was evaluated only in svchost.exe (Pid=752)
**********************************************************************
```

**Figure 18: Example of Parameter Usage**

**Table 2: Results of Study Regarding Generic IOCs**

| IOC Definition | Study Details | Limitations |
|---|---|---|
| Abnormal execution path | Detects executable files that contain folders not normally used often in their path, such as Recycle.Bin or Users\Public | Effective against processes that are running, but generates many false positives when used on access history |
| Web injection | Detects processes with all HttpSendRequest API hooked | Fails to detect some malware depending on the type of hooking carried out*67 |
| Code injection | Detects code-injected processes based on their memory space characteristics or the API used | Cannot detect wow64 processes*68 |
| Position Independent Code (PIC)*69 | Detects things such as code sequences of access to PEB*70 and GetPC*71, and immediate values of API name hashes | False positives occur for GetPC, and searching for API name hash values creates significant load |
| UAC prompt bypass | Detects code sequences that inhibit UAC prompts | Only one technique is defined, and there are other techniques for inhibiting this |
| Storage of data in a special area of NTFS | Detects processes and drivers that read and write to the NTFS Extended Attributes*72 | False positives occur when evaluating drivers |
| Lateral movement of targeted attacks | Detects attack tools used for lateral movement | Relies on metadata such as file names, so generic definitions are difficult |

*61 The detail parameter displays a character string in its entirety when a partial match is found. Specify “on” as the value. The note parameter is used when you want to add a comment for each term. Detailed configuration methods are explained on the following page (http://takahiroharuyama.github.io/blog/2014/10/24/openioc-parameters-used-by-openioc-scan/).

*62 An abbreviation of Direct Kernel Object Manipulation. In this case, it indicates processes hidden by altering the linked list of processes retained by the kernel.

*63 A registry value found in HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatibility\AppCompatCache or HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache\AppCompatCache.

*64 IRP is an abbreviation of I/O Request Packets. The function table for controlling the reading and writing of the buffer set for each driver is called the IRP function table.

*65 An abbreviation of System Service Descriptor Table. SSDT entries are system call names.

*66 MFT is an abbreviation of Master File Table. MFT entries are the metadata created for each file and folder managed using an NTFS file system.

*67 With regard to inline hooks, Volatility Framework only checks the first three instructions, so when a hook is embedded in the fourth instruction or later it cannot be detected.

*68 Due to the limitations of the virtual address translation system of Volatility Framework.

*69 Code that operates regardless of the execution context, such as shellcode.

*70 An abbreviation of Process Environment Block. Information required to access the API used.

*71 An abbreviation of Get Program Counter. Code for acquiring the current execution point.

*72 A data space used for compatibility with OS/2 applications.

priority to conduct analysis in further detail (triage), we feel that they can be utilized to a certain extent. Meanwhile, we also saw cases in which detection failed due to the limitations of the functions in Volatility Framework itself.

**■ Summary**

In this section we introduced openioc_scan, and presented the results of our study regarding generic IOCs using this. The study identified limitations derived from the functions in Volatility Framework, but as this tool is open source unlike Redline, each user is able to freely fix and extend these functions.

It seems there are still few analysts that utilize IOCs at all, let alone apply the concept of scanning memory images for IOCs. It is easy to predict that the number of computers subject to analysis in incident responses, as well as memory and disk drive capacity, will continue to increase steadily in the future. Experienced analysts may already feel that existing techniques have reached their limits. Try using openioc_scan to detect threats and perform triage, enabling more efficient incident response.

### 1.4.3 ID Management Technology

In 2014, the never ending stream of unauthorized login incidents thought to use lists of user IDs and passwords leaked in other incidents and accidents continued. As a result, there is growing awareness of the dangers of authentication methods that use only IDs and passwords, and new ID management technology that also incorporates other authentication methods has attracted attention. In this section, we examine this ID (identity) management technology. ID management technology involves more than technology related to the lifecycle, such as the issuing, usage, and disposal of IDs. It also encompasses an extremely diverse range of approaches, such as user authentication, issuing and usage of credentials, management and circulation of attribute information, access control for various resources, and delegation of authority, as well as technology for coordinating this information between different entities. Consequently, there are a wide variety of specifications related to the management and coordination of IDs used on the Internet. Because each is developed based on different concepts, it is necessary to select the one most appropriate for the environment it will be used in. However, due to the different technical terms used and the increasingly broad range that specifications cover, this is unfortunately becoming an extremely difficult area to understand. In this section, we aim to assist the implementation of technology by avoiding discussion of specific specifications whenever possible, and examining general approaches to ID management technology.

**■ Approaches to IDs - Entities and Identifiers**

When it comes to identity, there are an extremely large number of approaches, definitions, and concepts, and this is one of the factors that causes confusion among technical experts and users. For that reason, in this report we will take the simple approach of treating IDs as identifiers.

Entities in the real world are tied to entities in the digital world. One example of an entity in the real world is a user that is trying to use some kind of service, but as represented by the IoT (Internet of Things), devices that actively seek to connect to other nodes also sometimes have IDs. When this happens, a unique identifier is assigned to identify entities in the digital world. IDs can be thought of as the members of the identifier space determined for each individual realm. ID uniqueness means that different IDs are assigned to different entities in the corresponding realm.

It is typical for entities in the real world to have different IDs in a number of realms. Furthermore, entities in the real world are often associated with multiple IDs in the same realm. However, in the digital world, different IDs are recognized as different entities. For example, the real-world entity Mr. A may have the email addresses a@aaa.example and a@bbb.example, possessing IDs in the two different realms, aaa.example and bbb.example. Mr. A may also have different email addresses in the same domain in some cases, such as a1@aaa.example in addition to a@aaa.example in the aaa.example realm. This demonstrates that the same entity in the real world can have multiple IDs assigned in different realms in the digital world.

**■ Tokens/Credentials and Authentication**

As mentioned previously, using IDs in the digital world enables us to identify different entities. However, IDs are public information, and it would pose a problem if simply anyone could claim they were a particular entity. Consequently, an authentication system is required for verifying an entity that is requesting access really is the entity that ID was assigned to. For this, private information such as a password that matches the corresponding ID is needed.

Here, in line with the NIST SP800-63*73 definitions, we will explain credentials*74 and tokens separately. Tokens indicate information that should be kept secret held by users assigned the corresponding ID. They fall into the categories of "something you know," "something you have," or "something you are." Examples of tokens include passwords or the private keys used in public key cryptosystems, physical media such as IC cards or dongles, and body characteristics used for biometric authentication such as fingerprints or irises. Meanwhile, credentials are public information that indicate associations between tokens and IDs. In some cases credentials are signed by a trusted entity, and serve as information that a third party can verify the validity of. For password-type tokens, IDs can be thought of as credentials. Considering public key cryptosystem authentication methods used with protocols such as SSL/TLS, the X.509 certificate*75 is the credential, and the private key that matches the public key included in the certificate corresponds to the token. SSL/TLS server certificates also include the FQDN, and this can be thought of as an ID. Bitcoin addresses can be regarded as IDs, but because the address itself is a public key, and transaction signature verification can be performed using only the address, you can also regard them as credentials.

An authentication method using multiple [token/credential] pairs instead of a single pair to authenticate an entity with a certain ID assigned is called multi-factor authentication. The most widely-known method is parallel multi-factor authentication, in which independent tokens are used for each authentication method. Meanwhile, some opt for a cascading approach to multi-factor authentication. For example, when using a private key as a token in public key cryptosystems, the private key file is generally encrypted, so the password must be entered to decrypt it. The use of both the password and private key as tokens at this time can be regarded as cascading multi-factor authentication. The same applies to IC cards and PIN numbers. Additionally, for hardware tokens that fall into the "something you have" token category, a one-time password that is shown on the physical media and periodically updated is typically presented as a token, and used as a part of multi-factor authentication. For network environments, a one-time password system using Lamport's hash chains*76 is known, and has been drawn up in specifications*77*78 such as S/Key. One-time password systems show promise as a proposed countermeasure*79 for the list-based attacks of recent years, through replacement of or combined use with conventional ID/password systems.

### ■ Differences Between Authentication and Authorization

In the digital world, the ultimate aim is not for a user to login, or for a server to authenticate an entity with a certain ID. After a server identifies a user, authentication is performed to provide appropriate service or enable access to various resources. Once an entity is validated, the act of granting privileges to the entity with the corresponding ID is called authorization, and this is considered separately to authentication. Authorization merely grants the proper access privileges to a given ID. A policy is a prerequisite for this, and there is an approach in which roles are separated into an entity PDP (Policy Decision Point) that grants privileges to a given ID based on the policy, and an entity PEP (Policy Enforcement Point) that actually applies the determined results*80. Access control methods for granting privileges to a given ID include models such as RBAC (Role-Based Access Control)*81 and ABAC (Attribute-Based Access Control)*82. These methods take the approach of determining whether to grant privileges based on attribute information associated with an ID, instead of granting privileges to the ID directly. The main difference between these two methods is that RBAC handles attribute information with fixed attribute values called roles, and ABAC adopts a configuration method in which attribute information called an attribute takes a value within a given range, with privileges selected based on the range that this value belongs to. For example, the RBAC approach is to grant access privileges based on position or gender, while the ABAC approach is to grant them based on

*73 NIST Special Publication 800-63-2, Electronic Authentication Guideline (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf).
*74 The term credentials is sometimes used to refer collectively to all information used in authentication, but for its use in this report we think that clear classification should be made with regard to public information and private information.
*75 ITU-T Recommendation X.509 | ISO/IEC 9594-8, Information Technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks
*76 Lamport, "Password Authentication with Insecure Communication". Communications of the ACM 24.11, November 1981, pp.770-772.
*77 N. Haller, "The S/KEY One-Time Password System" (http://tools.ietf.org/html/rfc1760).
*78 N. Haller et al., "A One-Time Password System" (http://tools.ietf.org/html/rfc2289).
*79 Ministry of Internal Affairs and Communications, "A collection of list-based attack countermeasures" (http://www.soumu.go.jp/main_content/000265404.pdf) (in Japanese).
*80 OASIS, "eXtensible Access Control Markup Language3 (XACML) Version 2.0" (http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf).
*81 David Ferraiolo, Richard Kuhn, "Role-Based Access Controls", 15th National Computer Security Conference (http://csrc.nist.gov/rbac).
*82 NIST, Attribute Based Access Control (ABAC) Overview (http://csrc.nist.gov/projects/abac/).

ages or periods/times. The attribute information used for authorization is sometimes managed by the entity that assigns IDs and performs authentication. However, another method involves an entity that manages attribute information (an attribute authority) issuing credentials and associating IDs and attribute information. The benefit of circulating attribute information as credentials is that it protects against information not required under normal circumstances also being sent to service providers along with attribute information that a user should disclose to gain access privileges. As a result, only the minimal amount of attribute information is disclosed to receive service*83. Figure 19 is a conceptual diagram showing the flow from token-based authentication to the circulation of each type of credential and the granting of access privileges.

### ■ ID Federation Technology

There are a number of frameworks called ID federation for implementing single sign-on, which enables services in multiple realms to be used at the same time. Here we focus mainly on the SAML (Security Assertion Markup Language)*84 approach. The roles in SAML can be divided into (1) the IdP (identity provider) that conducts tasks related to ID assignment and authentication, (2) the RP (relying party) / SP (service provider) that trust and accept the credentials issued by the IdP, and (3) the end user. The end user presents their credentials when using the services of the SP. It is the IdP that issues these credentials. Based on the policy determined by the SP, credentials called assertions are requested, and issued by the IdP. In SAML, the protocol specifies the actions taken when a browser behaves as an end user, in addition to the data format for assertions. Regarding credential (assertion) types, it is possible to circulate information that guarantees attribute information, as well as information related to authorization decisions, in addition to information about authentication results. When doing this, as shown in Figure 19, it is possible to think of the organization issuing credentials relating to authentication as the IdP in a narrow sense, while breaking down the roles into the attribute authority that issues credentials regarding attribute information, and the PDP that issues credentials regarding authorization decisions. Furthermore, the SP serves as the PEP, but depending on the implementation it is also conceivable to omit the issuing of assertions by the PDP and have the SP handle the role of both PDP and PEP.

OpenID*85 is another framework based on concepts similar to SAML. The circulation of attributes is enabled using a system in which the RP verifies the credentials (called claims) issued by an entity called an OpenID Provider (OP), which plays the roles of narrowly interpreted IdP and attribute authority mentioned earlier. Operations are possible even when the OP and RP do not coordinate in advance, and an extension specification regarding discovery services for facilitating the discovery of the appropriate OP/RP by each RP/OP is also available. Furthermore, specifications for the delegation of authority have also been established, and OAuth*86 provides a system in which users with a token for accessing resources temporarily grant only privileges to a delegate without disclosing the private token information. This may be confusing as the technical terms are different, but users known as resource owners can enable delegates to access resources via a PDP called an authorization server, which issues credentials including authorization information called an access token without passing on private information.

*83 Additionally, there is also the approach of gaining access privileges using a pseudonym for the ID as well, but we do not cover this here.

*84 OASIS, Security Assertion Markup Language (SAML) (http://xml.coverpages.org/saml.html).

*85 OpenID Foundation, OpenID specifications (http://openid.net/developers/specs/). Previously formulated specification groups such as OpenID Authentication have been discontinued and incorporated in OpenID connect 1.0, which is based on OAuth 2.0.

*86 D. Hardt, "The OAuth 2.0 Authorization Framework" (http://tools.ietf.org/html/rfc6749). OAuth 2.0 specifications are established on the following page (http://tools.ietf.org/wg/oauth/).

In this way, we expect that a variety of specifications based on new models will continue to be established in the future. We hope that learning about general approaches to IDs, tokens, credentials and authentication, authorization, and access control as presented here will assist in the understanding of new specifications.

## 1.5 Conclusion

This report has provided a summary of security incidents to which IIJ has responded. In this report, we presented countermeasures against the alteration of domain name registration information, and looked at the openioc_scan plug-in that scans for threats lurking in the memory of a device. We also examined ID management technology. 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.

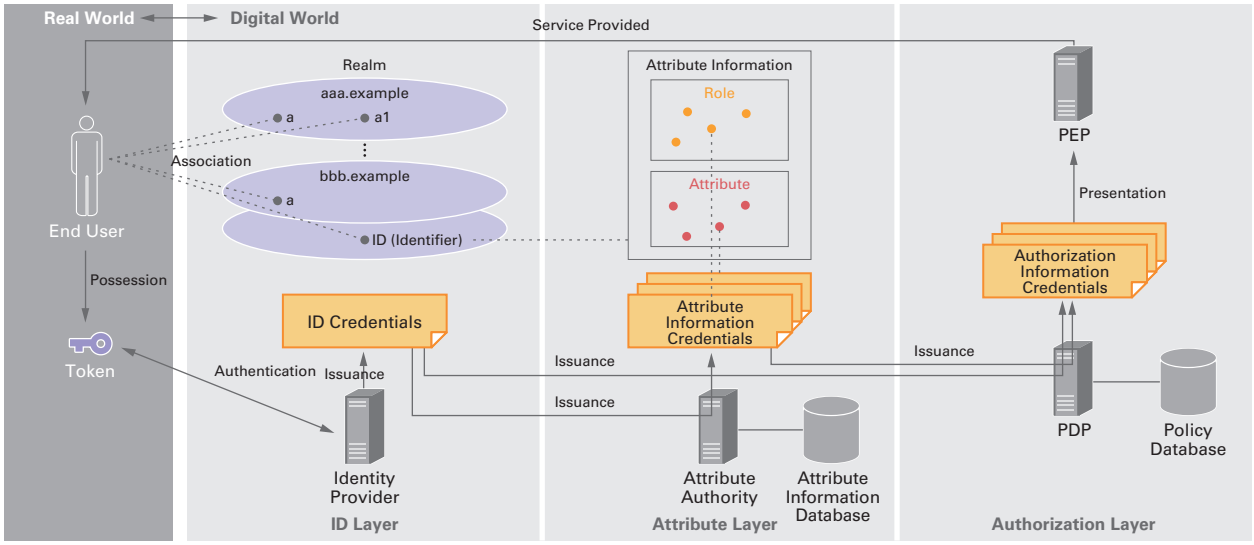



**Figure 19: Flow From Token-Based Authentication to Circulation of Credentials and Granting of Access Privileges**

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)
**Minoru Kobayashi** (1.4.1 Countermeasures Against the Alteration of Domain Name Registration Information)
**Takahiro Haruyama** (1.4.2 The openioc_scan Plug-in That Scans for Threats Lurking in Device Memory)
**Yuji Suga** (1.4.3 ID Management Technology)
Office of Emergency Response and Clearinghouse for Security Information, Service Operation Division, IIJ

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