The Shellshock Bash Vulnerability

In this report, we discuss the Shellshock Bash vulnerability, and look at the new POODLE attack method that targets SSLv3. We also examine the occurrence of a series of list-based attacks since last year, and go over some countermeasures for them.

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 July 1 through September 30, 2014. In this period a number of sites in Japan, including those for media outlets, were affected by DNS hijackings that led to malware infections. A vulnerability was also discovered in GNU Bash, affecting an extensive range of products and services. Unauthorized login incidents due to list-based attacks on online services continued to occur, as did incidents of illegal remittance stemming from the misuse of online banking. There were also SSDP-based DDoS attacks in Japan, coming in the wake of those that used DNS or NTP amplification. Outside Japan, there were sporadic DDoS attacks that exceeded 200 Gbps in bandwidth. 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 July 1 and September 30, 2014. Figure 1 shows the distribution of incidents handled during this period*1.

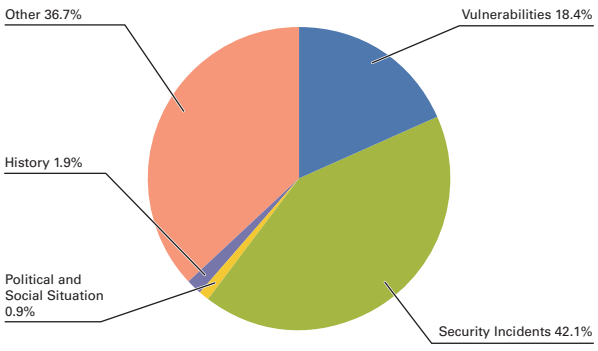


Figure 1: Incident Ratio by Category (July 1 to September 30, 2014)

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. Between July and August, website alterations, DDoS attacks, and information leaks affected a number of government-related sites and private-sector business websites in Israel, in relation to the conflict in Palestinian-controlled Gaza Strip (OpSaveGaza). Attacks were also made between other countries in conflict, such as Russia and Ukraine, India and Indonesia, and India and

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

Pakistan. Between August and September, there were protests against the Pakistani government in the form of website alterations, DDoS attacks, and information leaks through SQL injections that affected a number of government-related sites (OpPakistan). In September, there were DDoS attacks and leaks of email account information that affected websites of the Chinese government and the Hong Kong executive branch, in relation to demonstrations about issues with the electoral system in Hong Kong (OpHongKong).

Other attacks by hacktivists such as Anonymous continued on government and government-related websites around the world. Unknown attackers claiming affiliation with the Syrian Electronic Army continued to hijack SNS accounts and deface websites, with affected accounts including those for the Israel Defense Forces.

■ Vulnerabilities and their Handling

During this period, fixes were released for Microsoft's Windows*2*3 and Internet Explorer*4*5*6. Updates were also made to Adobe Systems' Adobe Flash Player, Adobe Reader, and Acrobat. A quarterly update was provided for Oracle's Java SE, fixing many vulnerabilities. Several of these vulnerabilities were exploited before patches were released. Regarding server applications, a quarterly update was released for a number of Oracle products, including the Oracle database server, fixing many vulnerabilities.

A number of vulnerabilities, including those that allowed elevation of privileges, were discovered and fixed in Cisco Unified Communications Domain Manager. One of the vulnerabilities fixed involved the use of the default SSH private key. Using the default SSH private key on a device without updating it leads to a high risk of exploitation by third parties with the same private key, so this should be avoided*7.

A vulnerability (CVE-2014-6271) that could allow arbitrary OS commands to be executed was discovered and fixed in the Bash shell used in Unix-based OSes such as Linux. This vulnerability, which was given the name Shellshock, became a problem because it affected a large number of applications and devices, such as Web servers that run CGI scripts, routers, and gateway products. See "1.4.1 The Shellshock Bash Vulnerability" for more information about this issue.

■ Unauthorized Login Through Identity Fraud

Since last year there have been many attempts to steal user IDs and passwords, and log in without authorization presumably using lists of these IDs and passwords. These attempts continued in the current survey period. A variety of sites were targeted in these attacks, including survey sites, e-commerce sites, support sites for logistics companies, sites for mobile phone companies, and SNS. In a number of these incidents tangible damage was caused, such as the exchange of site points for gift points on other sites without authorization. As this demonstrates, the threat from list-based attacks still persists. A range of companies are taking steps to enhance the security of authentication functions for Web services and applications, such as adding two-step authentication or relaxing restrictions on password length and usable characters. Because problems have also been identified with users reusing the same password, or setting simple passwords that are easy to guess*8, users must also be sure to follow safe practices. See "1.4.3 The Status of List-Based Attacks and Their Countermeasures" for more information.

*2 "Microsoft Security Bulletin MS14-038 - Critical: Vulnerability in Windows Journal Could Allow Remote Code Execution (2975689)" (https://technet.microsoft.com/library/security/ms14-038).

*3 "Microsoft Security Bulletin MS14-043 - Critical: Vulnerability in Windows Media Center Could Allow Remote Code Execution (2978742)" (https://technet.microsoft.com/library/security/ms14-043).

*4 "Microsoft Security Bulletin MS14-037 - Critical: Cumulative Security Update for Internet Explorer (2975687)" (https://technet.microsoft.com/library/security/ms14-037).

*5 "Microsoft Security Bulletin MS14-051 - Critical: Cumulative Security Update for Internet Explorer (2976627)" (https://technet.microsoft.com/library/security/ms14-051).

*6 "Microsoft Security Bulletin MS14-052 - Critical: Cumulative Security Update for Internet Explorer (2977629)" (https://technet.microsoft.com/library/security/ms14-052).

*7 See the IIJ Security Diary post, "The Issue of Many Public Keys Unintentionally Sharing Private Keys with Other Sites" (https://sect.iij.ad.jp/d/2012/08/109998.html) (in Japanese) for information on the risks of using the same private key.

*8 For example, see the IPA "Report on the 'Survey of Online Personal Authentication Systems'" (http://www.ipa.go.jp/security/fy26/reports/ninsho/index.html) (in Japanese).

July 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

V **3rd:** A number of vulnerabilities, including those that allowed elevation of privileges, were discovered and fixed in Cisco Unified Communications Domain Manager.
"Multiple Vulnerabilities in Cisco Unified Communications Domain Manager" (http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140702-cucdm).

V **9th:** Microsoft published their Security Bulletin Summary for July 2014, and released six updates, including the two critical updates MS14-037 and MS14-038, as well as three important updates.
"Microsoft Security Bulletin Summary for July 2014" (https://technet.microsoft.com/library/security/ms14-jul).

V **9th:** A number of vulnerabilities in Adobe Flash Player that could allow arbitrary code execution were discovered and fixed.
"APSB14-17: Security updates available for Adobe Flash Player" (http://helpx.adobe.com/security/products/flash-player/apsb14-17.html).

S **9th:** A correspondence education company announced that information on 20,700,000 of their customers had leaked to third parties including list traders. Later, in a final report published in September, it was revealed that the personal information of 48,580,000 customers had leaked.

S **9th:** It came to light that certificates for a number of Google and Yahoo! domains had been issued without authorization at the National Informatics Center of India (NIC), which operates an intermediate certificate authority affiliated with the root certificate authority of the government of India. As a result, these certificates were revoked in a number of browsers. It is thought that this happened when the certificate issuing process was compromised.
Google Online Security Blog, "Maintaining digital certificate security" (http://googleonlinesecurity.blogspot.jp/2014/07/maintaining-digital-certificate-security.html).

O **15th:** The Amended Act Prohibiting Child Prostitution and Pornography that was passed in June came into effect. However, regarding the provisions of Article 7-1 of the amended act, which details punishment for the possession of child pornography for the purpose of fulfilling personal sexual curiosity, a grace period of one year from enactment in which such material could be disposed of appropriately was given in an additional clause. This article will now apply from July 15, 2015.
See the following Ministry of Justice explanation for more details. "The bill for amending part of the Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children" (http://www.moj.go.jp/keiji1/keiji11_00008.html) (in Japanese).

O **15th:** The Ministry of Internal Affairs and Communications published its "Information and Communications in Japan 2014" white paper, which examines the current status of information and communications in Japan, as well as trends in information and communications policy.
Information and Communications White Paper Site (http://www.soumu.go.jp/johotsusintokei/whitepaper/index.html) (in Japanese).

V **16th:** Oracle released their quarterly scheduled update for a number of products including Oracle, fixing a total of 113 vulnerabilities, including 20 in Java SE.
"Oracle Critical Patch Update Advisory - July 2014" (http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html).

O **16th:** The IPA officially established its Cyber Rescue Squad to support organizations affected by targeted attacks. Their role will be to limit damages, deter and reduce reoccurrence, and implement swift countermeasures to prevent a chain reaction effect.
"Press Release - Cyber Rescue Squad Established to Support Countermeasures to Targeted Attacks (https://www.ipa.go.jp/about/press/20140716_1.html) (in Japanese).

S **17th:** Regarding an incident in which customer information was leaked from a correspondence education company, a former temporary employee of a subcontractor was arrested on suspicion of violating the Unfair Competition Prevention Act (copying of trade secrets).

S **18th:** The Telecom Information Sharing and Analysis Center Japan announced it would issue alerts to users affected by a type of malware that targets Internet banking (Gameover Zeus) through its public-private project to support malware countermeasures in Japan (ACTIVE), as part of an international operation to remove infections.
"Regarding Alerts for Users Infected with Malware That Targets Internet Banking" (https://www.telecom-isac.jp/news/news20140718.html) (in Japanese).

O **22nd:** The Council for Stable Operation of the Internet published the third edition of its "Guidelines for Dealing with High Volume Communications and Privacy at Telecommunications Carriers."
"Guidelines for Dealing with High Volume Communications and Privacy at Telecommunications Carriers (Third Edition)" (http://www.jaipa.or.jp/other/mtcs/guideline_v3.pdf) (in Japanese).

O **23rd:** The Ministry of Internal Affairs and Communications announced it would hold a "Workshop on Personal Data Held by Government Institutions, etc." to investigate and evaluate the possible use and protection of personal data in the possession of government institutions and independent administrative agencies.
"Workshop on Personal Data Held by Government Institutions, etc." (http://www.soumu.go.jp/main_sosiki/kenkyu/gyousei_personal/index.html) (in Japanese).

S **24th:** The European Central Bank announced its website had been compromised, and that personal data including the email addresses of event registrants had leaked. This incident came to light when an anonymous email demanding money in return for the leaked data was received.
See the following European Central Bank announcement for more details. "24 July 2014 - ECB announces theft of contact information" (https://www.ecb.europa.eu/press/pr/date/2014/html/pr140724.en.html).

S **25th:** A number of companies and government institutions in Japan issued a series of alerts regarding websites that imitated their own sites.

V **29th:** Fixes were made to a vulnerability in a number of IP cameras that allowed authentication to be bypassed, leading to the possibility of arbitrary operations being executed by obtaining device configuration details such as authentication information.
JVN, "JVNDB-2014-000087 Multiple I-O DATA IP Cameras vulnerable to authentication bypass" (http://jvndb.jvn.jp/en/contents/2014/JVNDB-2014-000087.html).

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

*Dates are in Japan Standard Time

■ Website Alterations and Redirection to Malware

During this survey period, there continued to be many incidents in which websites were altered to redirect visitors to malicious software. There were website alterations and resulting redirection to malware at a tour company, an automobile sales company, and a security firm. In addition to redirection to malware sites, in an incident in which the website of an independent administrative agency was altered, there were attempts to exploit it as a phishing site*9. A text editing software support site was also altered, redirecting users accessing it to another site where malware was installed. After the incident came to light, it was revealed that the content of a legitimate update file was also altered in an attempt to get users to install a virus-infected file. We believe this kind of malware infection activity that exploits update systems for legitimate software will continue in the future.

■ Attacks Based on Political and Social Situation and Historical Context

During this period each year there are incidents related to historical dates in the Pacific War, as well as Takeshima and the Senkaku Islands. We stayed vigilant, as this year it was expected that the websites of a number of government agencies and private-sector businesses in Japan would be subject to alterations through compromise via SQL injections and brute force attacks, as well as DDoS attacks, in relation to these sensitive issues. However, although there was an increase in unauthorized access through SQL injection attacks in some cases*10, and website alterations also took place*11, no large-scale attacks were confirmed. IIJ's observations showed slightly more DDoS attacks than usual, but the number and scale of attacks was significantly lower than the same period in previous years.

■ DDoS Attacks

A number of large-scale DDoS attacks occurred during this period. In August, an individual or group calling themselves the Lizard Squad attacked a number of game-related servers, including those for PSN, Xbox Live, and League of Legends. The incident affecting PSN is thought to have involved an NTP reflection attack of 263.35 Gbps. In addition to DDoS attacks, the perpetrator also made claims online that they had placed a bomb on the plane an executive was flying in, leading to the flight being diverted. Attacks on game-related servers thought to be the work of this attacker also continued intermittently in September. In Japan, periodic DDoS attacks were made on the DNS servers of a number of ISPs in late May, and these continued through to July at some ISPs. In September, a high school student was referred to prosecutors on the charge of obstruction of business by damaging a computer, having been suspected of attacking game servers in March using an overseas DDoS attack service.

■ Malware Infections and Information Leaks at Companies

During this survey period, there were ongoing incidents of large-scale leaks of data including customer information due to corporate systems being infected with malware. In particular, it was announced in August that 51 domestic branches of a major U.S. logistics company had been infected with malware, leading to the possibility that details such as customer credit card information had been leaked. There were also incidents in Japan, including malware infections of terminals at an airline company, which could have resulted in customer information being sent to an external party and leaked. In September, there was an incident at a major home improvement center company in which the details of approximately 56 million payment cards and email addresses may have leaked. It is thought that a variant of the malware targeted at POS systems that has been active since last year was used in this incident, and data including credit card information could have leaked. Information leaks due to malware also took place at a number of other companies, including hospitals and retailers. Due to POS malware in particular causing multiple large-scale information leaks since around the end of last year, US-CERT issued a number of alerts*12. New POS malware variants continue to appear*13, so ongoing vigilance will be necessary.

*9 For example, see the following National Research Institute for Earth Science and Disaster Prevention announcement. "Regarding Alterations to the NIED Website" (http://www.bosai.go.jp/press/2014/pdf/20140811_01.pdf) (in Japanese).

*10 For example, it has been reported in IBM's Tokyo SOC Report that attacks such as SQL injections from specific countries are on the rise. "Attack trends around September 18 when the Liutiaohu Incident took place" (https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/201409attackfromcn?lang=en_us) (in Japanese).

*11 See the following F-Secure blog post for more information. "Sept. 18 cyber attacks (follow-up)" (http://blog.f-secure.jp/archives/50734688.html) (in Japanese).

*12 US-CERT issues ongoing alerts, such as "TA14-002A: Malware Targeting Point of Sale Systems" (https://www.us-cert.gov/ncas/alerts/TA14-002A) in January and "Alert (TA14-212A) Backoff Point-of-Sale Malware" (https://www.us-cert.gov/ncas/alerts/TA14-212A) in August.

*13 For example, see the Trend Micro blog post "2014 - An Explosion of Data Breaches and PoS RAM Scrapers" (http://blog.trendmicro.com/trendlabs-security-intelligence/2014-an-explosion-of-data-breaches-and-pos-ram-scrapers/) for more information.

August Incidents

1st: US-CERT issued an alert regarding a newly discovered type of malware called Backoff that targets POS systems.
"Alert (TA14-212A) Backoff Point-of-Sale Malware" (https://www.us-cert.gov/ncas/alerts/TA14-212A).

1st: Microsoft released the Enhanced Mitigation Experience Toolkit (EMET) 5.0, which is a security tool for mitigating application vulnerabilities.
See the following TechNet Blogs post for more information. "Announcing EMET 5.0"
(http://blogs.technet.com/b/srd/archive/2014/07/31/announcing-emet-v5.aspx).

2nd: The Mozilla Developer Network announced that 76,000 MDN user email addresses and 4,000 encrypted user passwords may have leaked due to a database dump file being mistakenly made available to the public.
Mozilla Developer Network, "MDN Database Disclosure" (https://blog.mozilla.org/security/2014/08/01/mdn-database-disclosure/).

4th: There was an incident of unauthorized access at Gamma International, the provider of the FinSpy (FinFisher) commercial surveillance software allegedly used by government institutions around the world for intelligence gathering activities. As a result, a total of 40 GB of internal documents and source code was released.

8th: A U.S. security company reported that BGP hijacking attacks had been used to redirect traffic destined for a virtual currency mining pool to a fake mining pool between February and May 2014. It is thought that 19 ISPs were affected by these attacks, and the attacker may have profited by as much as $83,000.
See the following Dell SecureWorks blog post for more information. "BGP Hijacking for Cryptocurrency Profit"
(http://www.secureworks.com/cyber-threat-intelligence/threats/bgp-hijacking-for-cryptocurrency-profit/).

12th: In the United States, a phenomenon that caused Internet speeds to drop and communications to become unstable occurred. This is thought to have been due to the advertised BGP routing information exceeding the maximum BGP routing table size of 512 k on older routers.
See the following BGPmon.net blog post for more information. "What caused today's Internet hiccup"
(http://www.bgpmon.net/what-caused-todays-internet-hiccup/).

13th: Microsoft published their Security Bulletin Summary for August 2014, and released two critical updates, MS14-043 and MS14-051, as well as seven important updates.
"Microsoft Security Bulletin Summary for August 2014" (https://technet.microsoft.com/library/security/ms14-aug).

13th: A number of vulnerabilities in Adobe Flash Player that could allow arbitrary code execution were discovered and fixed.
"APSB14-18: Security updates available for Adobe Flash Player" (http://helpx.adobe.com/security/products/flash-player/apsb14-18.html).

13th: A vulnerability in Adobe Reader and Acrobat that could allow remote arbitrary code execution was discovered and fixed.
"Security updates available for Adobe Reader and Acrobat" (http://helpx.adobe.com/security/products/reader/apsb14-19.html).

13th: It was announced that the Japanese and Simplified Chinese support sites for a text editor application had been altered, and traces of attempts to steal user names, passwords, and IP addresses were found. The website was subsequently altered again on August 18, and the update checking function of the shareware product was used to install malicious files in some cases.

15th: Microsoft published a recommendation to uninstall the MS14-045 update released in August 2014 as a preventative measure, even if no issues were experienced, due to the possibility of it causing abnormal shutdowns or boot failures when applied.
For more information, see the following explanation from the Japan security team's official blog "[Issue found after release] Installing the update released on August 13, 2014 may cause issues" (http://blogs.technet.com/b/jpsecurity/archive/2014/08/16/2982791-knownissue3.aspx) (in Japanese).

21st: U.S. UPS announced it had confirmed malware infections at 51 of its domestic branches, and that data such as the credit card information of its customers may have leaked.
See the following United Parcel Service of America, Inc. announcement for details. "The UPS Store, Inc. Notifies Customers Of Potential Data Compromise and Incident Resolution" (http://www.pressroom.ups.com/Press+Releases/Archive/2014/Q3/The+UPS+Store%2C+Inc.+Notifies+Customers+Of+Potential+Data+Compromise+and+Incident+Resolution).

25th: The PlayStation Network (PSN) and Sony Entertainment Network (SEN) were targeted in DDoS attacks carried out by an unknown party, causing major faults.
See the following PlayStation.Blog post for more information. "Update: PlayStation Network is Back Online"
(http://blog.us.playstation.com/2014/08/24/playstation-network-update-2/).

28th: Microsoft fixed and rereleased MS14-045, which had caused issues such as abnormal shutdowns and boot failures after being applied.
"Microsoft Security Bulletin MS14-045 - Important: Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege (2984615)"
(https://technet.microsoft.com/library/security/ms14-045).

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

*Dates are in Japan Standard Time

Government Agency Initiatives

Government agency initiatives included holding the 40th assembly of the government's Information Security Policy Council. The council published the "Annual Report on Cyber Security Policy (Fiscal 2013)," their first annual report that summarizes the overall status of cyber security in Japan for fiscal 2013, including the status of relevant policy at government institutions, critical infrastructure providers, and ministries, as well as related documents. Decisions were also made on "Cyber Security 2014," which compiles information such as the cyber security policies at each ministry for the current fiscal year*14.

Based on the "Policy Outline of the Institutional Revision for Utilization of Personal Data" that was published in June of this year, the Ministry of Internal Affairs and Communications held a "Workshop on Personal Data Held by Government Institutions, etc.," to investigate and evaluate the possible use and protection of personal data in the possession of government institutions and independent administrative agencies. They also published their "Location Information Privacy Report - Appropriately Protecting Location Information Privacy While Allowing Its Social Use and Application," which summarizes the proper handling of the acquisition and use of location information, as well as its provision to third parties*15. The aim of this report is to appropriately protect the confidentiality of communications, personal information, and privacy regarding the location information handled by telecommunications carriers, while promoting its social use and application, including for business purposes.

The National Police Agency published their White Paper on Police for 2014, which stated they had made a record number of arrests for cybercrimes, and indicated a big surge in the number of illegal remittances via Internet banking. The report also discussed initiatives such as their efforts to promote public and private coordination with regard to threats in cyberspace.

Other

Since June, countermeasures have been carried out for the Gameover Zeus malware that steals online banking information*16. In July, it was announced that information regarding terminals infected with this malware obtained through the operation would be used to provide ISPs with the details of infected parties, and alerts would be issued using this information*17. Additionally, progress is being made towards building a framework for international collaboration. One example of this is the establishment of a Joint Cybercrime Action Taskforce (J-CAT) by the European Police Office (Europol) in September*18. The task force covers a number of regions including Europe, the United States, and Canada, and its purpose is to deal with international cybercrime such as the examples above.

In July, a range of organizations and companies issued alerts regarding counterfeit websites*19. In August, government institutions also issued alerts regarding similar incidents. It is thought that these incidents originated from a Web proxy service, and did not target specific companies or organizations. Similar examples include those originating from a website conversion proxy provided by a mobile telecommunications carrier in China last year*20. Many other similar services are available, but because it is often not clear who the provider is, caution must be exercised when using them*21.

Also in July, the leak of customer information from a correspondence education company came to light. The incident was uncovered when another company sent direct mail based on the list of names obtained. A former temporary employee of a subcontractor of the affected company was arrested and charged with violating the Unfair Competition Prevention Act (copying of trade secrets), on suspicion of taking the data without authorization and selling it to list traders, etc.

---

*14 National Information Security Center, "Information Security Policy Council - 40th Assembly" (July 10, 2014) (http://www.nisc.go.jp/conference/seisaku/index.html#seisaku40) (in Japanese).

*15 Ministry of Internal Affairs and Communications, "Investigative Commission on the Handling of Location Information in Emergencies' 'Location Information Privacy Report - Appropriately Protecting Location Information Privacy While Allowing Its Social Use and Application' Report Published" (http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000144.html) (in Japanese).

*16 Department of Justice, "U.S. Leads Multi-National Action Against 'Gameover Zeus' Botnet and 'Cryptolocker' Ransomware, Charges Botnet Administrator" (http://www.justice.gov/opa/pr/2014/June/14-crm-584.html).

*17 Telecom Information Sharing and Analysis Center Japan, "Regarding Alerts for Users Infected with Malware That Targets Internet Banking" (https://www.telecom-isac.jp/news/news20140718.html) (in Japanese).

*18 See the following European Central Bank announcement for more details. "EXPERT INTERNATIONAL CYBERCRIME TASKFORCE IS LAUNCHED TO TACKLE ONLINE CRIME" (https://www.europol.europa.eu/content/expert-international-cybercrime-taskforce-launched-tackle-online-crime).

*19 For example, see the following Osaka Prefectural Police announcement, "Urgent: Beware of Imitations of the Osaka Prefectural Police Website!" (http://www.police.pref.osaka.jp/15topics/caution_domain.html) (in Japanese).

*20 See the following JPCERT Coordination Center tweet for more information (https://twitter.com/jpcert/status/322282948554530816) (in Japanese).

*21 See the following Trend Micro blog post for more information about this incident, "What lessons can be learned from the imitative site confusion caused by proxy avoidance systems?" (http://blog.trendmicro.co.jp/archives/9713) (in Japanese).

September Incidents

S **1st:** In the U.S., the personal photos of celebrities including Hollywood actresses were posted to a message board. It is thought that this incident originated from unauthorized access to the iCloud accounts of a number of celebrities that had leaked.
Apple published the following report on their investigation. "Apple Media Advisory Update to Celebrity Photo Investigation" (http://www.apple.com/pr/library/2014/09/02Apple-Media-Advisory.html).

O **1st:** The Ministry of Internal Affairs and Communications published its "Telecommunications Service Accident Status Report (2013)," which summarized the status of telecommunications accident reports for 2013.
"Telecommunications Service Accident Status Report (2013) (http://www.soumu.go.jp/menu_news/s-news/01kiban05_02000072.html) (in Japanese).

S **3rd:** A large-scale leak of card information occurred at major U.S. retailer The Home Depot.
See the following announcement from The Home Depot for more details. "The Home Depot Reports Findings in Payment Data Breach Investigation" (https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf).

O **4th:** The National Police Agency announced its statistics on unauthorized remittance crimes via Internet banking for the first half of 2014. These indicated that the total amount of money involved had surpassed the second half of 2013, and the scope of these incidents had spread to regional banks, credit unions, and credit associations. They also showed there was a sharp rise in incidents affecting corporate accounts.
"Status of Incidents of Illegal Remittance Related to Internet Banking in the First Half of 2014" (http://www.npa.go.jp/cyber/pdf/H260904_banking.pdf) (in Japanese).

V **10th:** Microsoft published their Security Bulletin Summary for September 2014, and released the MS14-052 critical update, as well as three important updates.
"Microsoft Security Bulletin Summary for September 2014" (https://technet.microsoft.com/library/security/ms14-sep).

V **10th:** A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB14-21: Security updates available for Adobe Flash Player" (http://helpx.adobe.com/security/products/flash-player/apsb14-21.html).

O **11th:** The National Police Agency published its "Report on Cyberspace Threats for the First Half of 2014," which gave an overview of trends in cybercrime for the first half of 2014.
"Report on Cyberspace Threats for the First Half of 2014" (http://www.npa.go.jp/kanbou/cybersecurity/H26_kami_jousei.pdf) (in Japanese).

V **17th:** A number of vulnerabilities in Adobe Reader and Acrobat that could allow unauthorized termination and remote arbitrary code execution were discovered and fixed.
"APSB14-20: Security updates available for Adobe Reader and Acrobat" (http://helpx.adobe.com/security/products/reader/apsb14-20.html).

S **18th:** A number of DDoS attacks were carried out on game servers, and a high school student was referred to prosecutors on suspicion of obstructing business by damaging a computer to interfere with game company operations.

P **18th:** Attacks often occur around this day each year for historical reasons. However, although there were small-scale attacks this year, no organized attacks were observed.

O **22nd:** LINE Corporation made it compulsory to set a PIN number (four digits) for smartphone versions of the LINE app, as a countermeasure to limit damages from frequent LINE account hijackings.
See the following official LINE blog post for more information "[Important] PIN numbers will be made compulsory to prevent the spread of unauthorized login (hijacking) incidents" (http://official-blog.line.me/ja/archives/1009539887.html) (in Japanese).

S **24th:** It was announced that unauthorized access had taken place at an airline company due to a malware infection, leading to the possibility that the personal information of up to 730,000 members had leaked.

V **25th:** A vulnerability in Bash that allowed arbitrary code execution was discovered and fixed. This fix was subsequently found to be insufficient, so further fixes were made for a number of vulnerabilities.
CERT/CC, "Vulnerability Note VU#252743 - GNU Bash shell executes commands in exported functions in environment variables" (http://www.kb.cert.org/vuls/id/252743).

V **26th:** A major cloud provider made news when they carried out large-scale maintenance due to an undisclosed vulnerability in Xen. On October 2, it was announced that this was to deal with CVE-2014-7188.
See the following Xen Project Blog post for more information. "XSA-108: Additional Information from the Xen Project" (https://blog.xenproject.org/2014/10/02/xsa-108-additional-information-from-the-xen-project-2/).

S **26th:** It was announced that unauthorized login thought to be a password list attack had targeted the support site for a logistics company, and the personal information of some members may have leaked through being viewed there.
A similar incident took place at another logistics company on the 28th.

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

*Dates are in Japan Standard Time

Revisions were made to the "Guidelines for Dealing with High Volume Communications and Privacy at Telecommunications Carriers," which are designed to help telecommunications carriers identify and deal with high volume communications such as DoS. The guidelines were then published by five telecommunications carrier organizations*22. The revisions were made based on the initial report of the Ministry of Internal Affairs and Communications' Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business, which was published in April*23. They incorporated measures for dealing with new threats such as DNS amplification attacks.

Also, from early September through to October, the .com domains used by a number of organizations in Japan were targeted in DNS hijackings, leading to attempts to install malicious software*24. Because these incidents involved the name server information registered to the registry being rewritten by some means to redirect traffic to a fraudulent website prepared by the attacker, JPCERT/CC and JPRS issued alerts*25.

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 July 1 and September 30, 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:

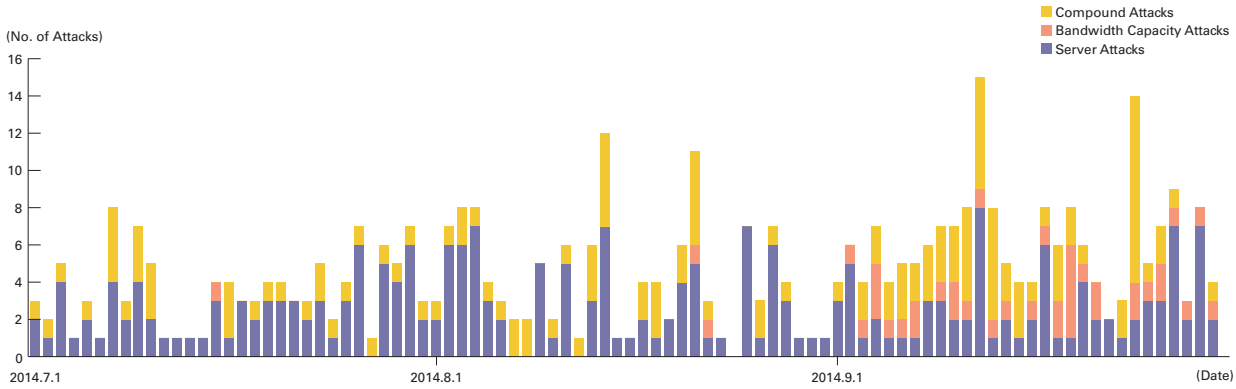


Figure 2: Trends in DDoS Attacks

*22 The Council for Stable Operation of the Internet is comprised of five industry associations with links to the telecommunications business. Refer to the website below for details on the establishment of these guidelines. Japan Internet Provider's Association (JAIPA) "Revision to Guidelines for Dealing with High Volume Communications and Privacy at Telecommunications Carriers" (http://www.jaipa.or.jp/topics/?p=695)(in Japanese).

*23 Ministry of Internal Affairs and Communications, "'Initial Report of the Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business' and Results of Request for Public Comment Published" (http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000074.html) (in Japanese).

*24 Volexity Blog, "Democracy in Hong Kong Under Attack" (http://www.volexity.com/blog/?p=33).

*25 Japan Registry Services (JPRS), "(Urgent) Regarding domain name hijackings caused by unauthorized rewriting of registered information and their countermeasures (published November 5, 2014) (http://jprs.jp/tech/security/2014-11-05-unauthorized-update-of-registration-information.html). (in Japanese).

attacks on bandwidth capacity*26, attacks on servers*27, and compound attacks (several types of attacks on a single target conducted at the same time).

During the three months under study, IIJ dealt with 340 DDoS attacks. This averages to 3.7 attacks per day, indicating a decrease in the average daily number of attacks compared to our prior report. Server attacks accounted for 71.5% of all incidents, while compound attacks accounted for 16.8%, and bandwidth capacity attacks 11.8%.

The largest attack observed during the period under study was classified as a compound attack, and resulted in 4.88 Gbps of bandwidth using up to 486,000 pps packets.

Of all attacks, 90.9% ended within 30 minutes of commencement, 9.1% lasted between 30 minutes and 24 hours, and none lasted over 24 hours. The longest sustained attack was a compound attack that lasted for 17 hours and 36 minutes.

Each year during this period, many DDoS attacks are observed around historic dates. From the beginning of September there was an increase in DDoS attacks, and a change was also seen in attack trends, but because these were not organized attacks, we couldn't link them to any particular cause.

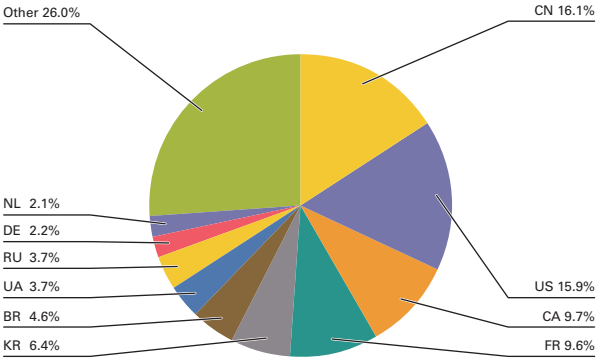


Figure 3: DDoS Attack Targets by Country According to Backscatter Observations

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*28 and botnet*29 usage as the method for conducting DDoS attacks.

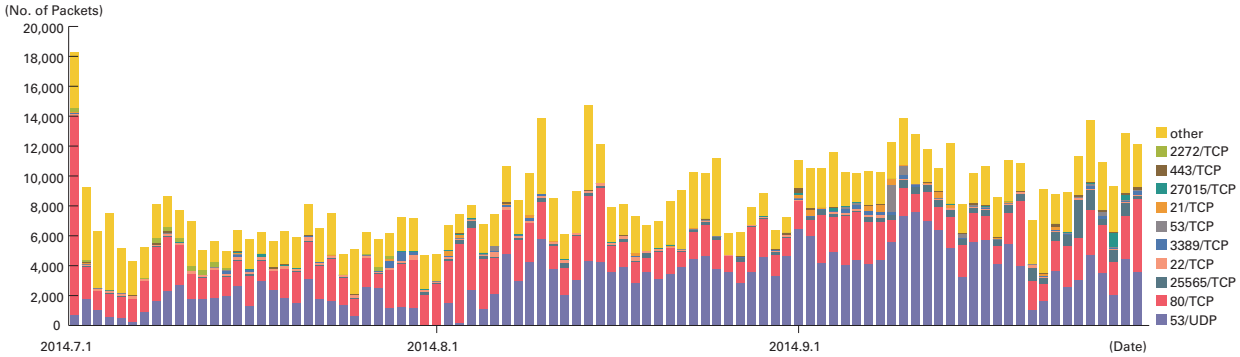


Figure 4: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)

*26 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.

*27 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.

*28 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.

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

■ Backscatter Observations

Next we present our observations of DDoS attack backscatter using the honeypots*30 set up by the MITF, a malware activity observation project operated by IIJ*31. 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 July 1 and September 30, 2014, Figure 3 shows the sender's IP addresses classified by country, and Figure 4 shows trends in packet numbers by port.

The port most commonly targeted by the DDoS attacks observed was the 53/UDP port used for DNS, accounting for 36.2% of the total during the target period. This was followed by 80/TCP used for Web services at 27.3%, so the top two ports accounted for 63.5% of the total. Attacks were also observed on 53/TCP used for DNS, 22/TCP used for SSH, 3389/TCP used for remote desktop, 21/TCP used for FTP, and 443/TCP used for HTTPS, as well as 25565/TCP, 27015/TCP, and 2272/TCP, which are not normally used.

The 53/UDP backscatter that has been on the increase since February this year continued to climb in the current survey period, becoming the port with the highest number of packets observed. Most of these packets show characteristics of the attack method known as DNS Water Torture*32. Additionally, the senders' addresses for the packets observed cover a wide range.

Regarding particularly large numbers of backscatter packets observed by port, there were attacks on the Web servers (80/TCP) of a television station in Ukraine between July 23 and August 15, and on the servers of a hosting provider in Russia between July 1 and July 24. In the latter case in particular, attacks had been continuing since June 16, in the last survey period. In September, many attacks on 25565/TCP were observed. This port is sometimes used with the servers for certain games. These attacks covered a wide range of targets, including those observed on a number of servers of a hosting provider in Russia. Between September 9 and September 10, attacks were observed on DNS (53/TCP) targeting a number of DNS servers that cover the .pk zone for Pakistan domains.

Notable DDoS attacks during the current survey period that were detected via IIJ's observations of backscatter included those between July and early August on sites related to the Israeli government thought to have been carried out by Anonymous.

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the MITF*33, a malware activity observation project operated by IIJ. The MITF uses honeypots*34 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.

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

*31 The mechanism and limitations of this observation method, as well as some of the results of IIJ's observations, are presented in Vol.8 on 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."

*32 Secure64 Software Corporation, "Water Torture: A Slow Drip DNS DDoS Attack" (https://blog.secure64.com/?p=377). For an explanation in Japanese, see the following document written by Mr. Morishita of Japan Registry Services. "DNS Water Torture Attacks" (http://2014.seccon.jp/dns/dns_water_torture.pdf) (in Japanese).

*33 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.

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

■ Status of Random Communications

Figure 5 shows the distribution of sender's IP addresses by country for communications coming into the honeypots between June 1 and September 30, 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 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 survey period, a large volume of 53/UDP communications occurred on July 27, August 14, and September 12. Most of these packets were caused by the receipt of DNS water torture packets, as mentioned in our backscatter observations*35. A small number of queries ranging from one to several were sent to each honeypot from a large number of IP addresses allocated mainly to the United States, Canada, and China. From this trend, we estimate that the attacker used a method such as a botnet. The queries contained A record resolution requests for "(random string).(existing domain)." On September 8, communications targeting 3395/UDP were made to the IP address of a specific honeypot from an IP address allocated to Iran. Upon investigating these communications, we found that random data from several dozen to several hundred bytes in length had been sent.

■ Malware Network Activity

Figure 7 shows the distribution of the specimen acquisition source for malware during the period under study, while Figure 8 shows trends in the total number of malware specimens acquired. Figure 9 shows trends in the number of unique specimens. In Figure 8 and Figure 9, the number of acquired specimens show the total number of specimens acquired per day*36, while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*37. 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.

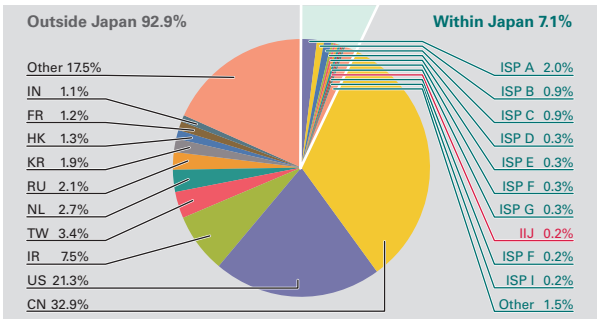


Figure 5: Sender Distribution (by Country, Entire Period under Study)

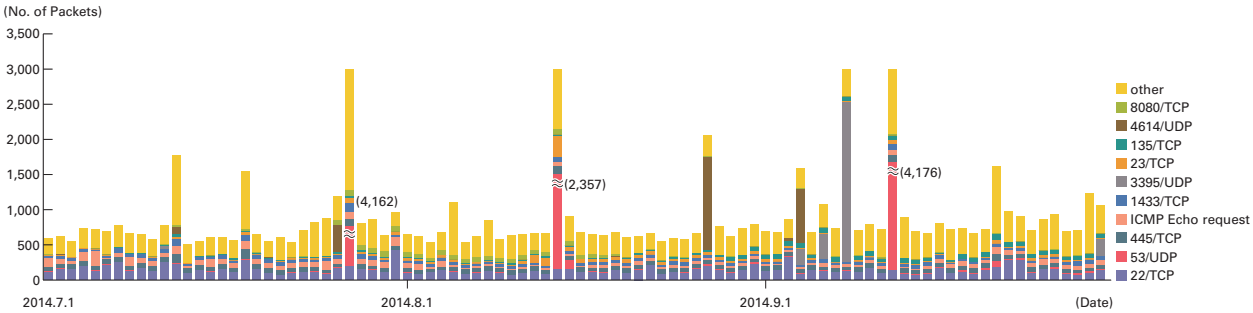


Figure 6: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

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

*36 This indicates the malware acquired by honeypots.

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

On average, 93 specimens were acquired per day during the period under study, representing 20 different malware. After investigating undetected specimens more closely, malware that steals passwords was observed from IP addresses allocated to Singapore and the Philippines. 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 96.0% of malware specimens acquired were worms, and 4.0% were downloaders. In addition, the MITF confirmed the presence of 1 botnet C&C server*38 and 16 malware distribution sites.

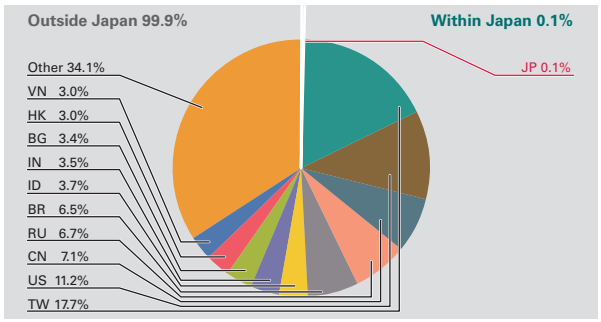


Figure 7: Distribution of Acquired Specimens by Source (by Country, Entire Period under Study, Excluding Conficker)

Conficker Activity

Including Conficker, an average of 25,435 specimens were acquired per day during the period covered by this report, representing 672 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 decreased by approximately 20% compared to the previous survey period. Unique specimens were also down

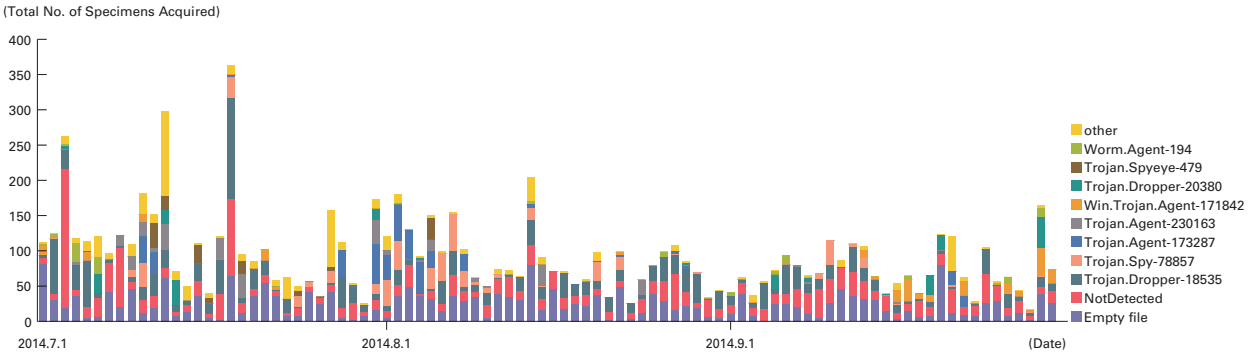


Figure 8: Trends in the Total Number of Malware Specimens Acquired (Excluding Conficker)

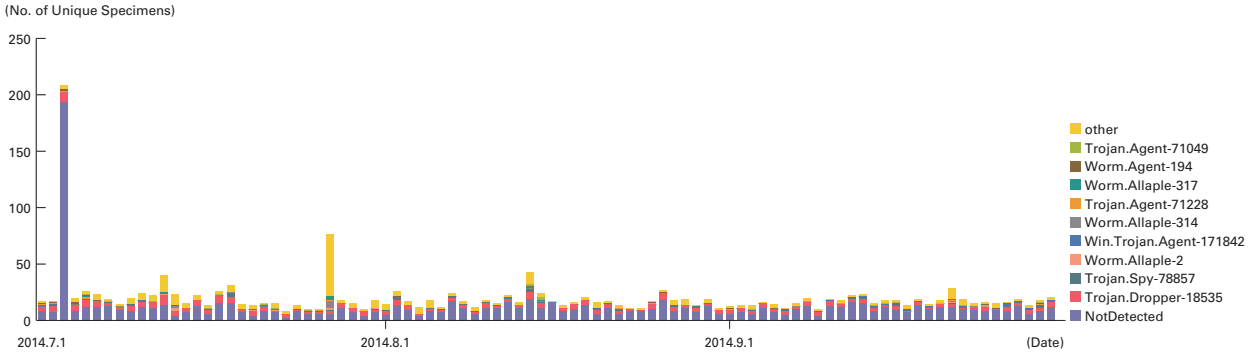


Figure 9: Trends in the Number of Unique Specimens (Excluding Conficker)

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

by about 7%. According to the observations of the Conficker Working Group*39, as of September 30, 2014, a total of 1,026,417 unique IP addresses are infected. This indicates a drop to about 32% of the 3.2 million PCs observed in November 2011, but it demonstrates that infections are still widespread.

1.3.3 SQL Injection Attacks

Of the types of different Web server attacks, IIJ conducts ongoing surveys related to SQL injection attacks*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 July 1 and September 30, 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.

China was the source for 48.2% of attacks observed, while the United States and Japan accounted for 20.5% and 11.3%, respectively, with other countries following in order. There was a dramatic increase in the number of SQL injection attacks against Web servers compared to the previous report. This was due to a significant spike in attacks originating from China.

During this period, attacks from a specific attack source in China directed at specific targets took place on July 19. On August 25, attacks were made from a number of sources in the United States directed at specific targets. On September 8, there were large-scale attacks from specific attack sources in China directed at specific targets. Attacks from a specific attack source in China directed at specific targets also took place on September 23. These attacks are thought to have been attempts to find vulnerabilities on Web servers.

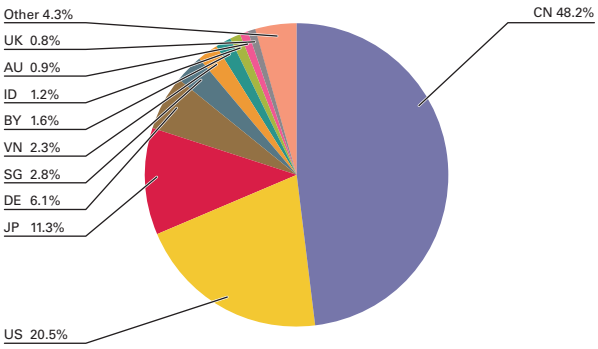


Figure 10: Distribution of SQL Injection Attacks by Source

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

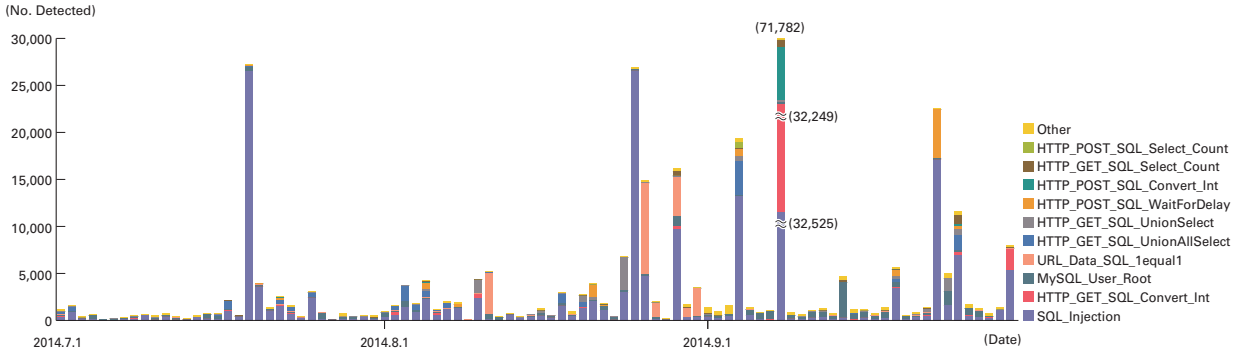


Figure 11: Trends in SQL Injection Attacks (by Day, by Attack Type)

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

*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.

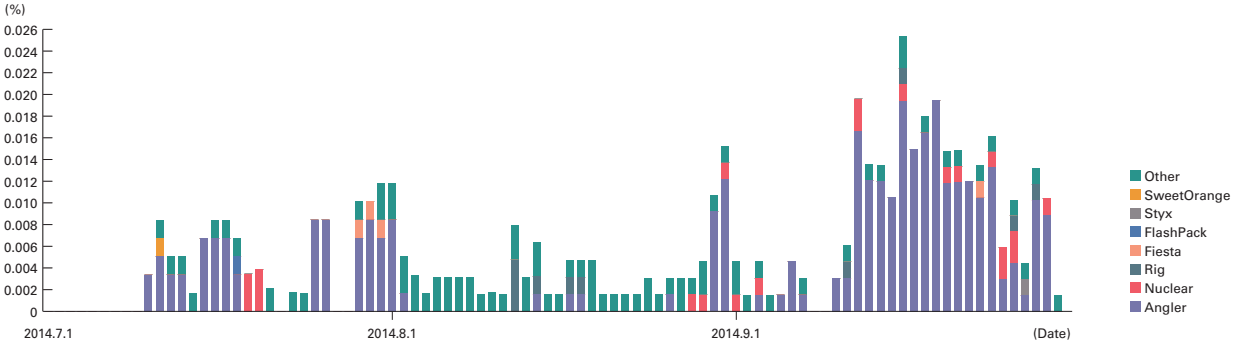
In the period from July to September, 2014, drive-by downloads were observed about twice as often as for the April to June period (Figure 12). As with the previous survey period, most of the attacks were based on Angler and Nuclear. Each of these exploit kits have functions for exploiting vulnerabilities in plug-ins such as Java, Flash, and Silverlight. In particular, functions have been added to Angler at a dizzying pace, and in late August a system that attempts to avoid detection by anti-virus software by not saving malware files on the client's hard disk during infection was discovered*42.

Also, after the attack detection logic of our Web crawler system was partially improved in mid-September, the number of Angler cases observed rose considerably. From this, we can surmise that although Angler appeared to have been wiped out in August, it is highly likely that attacks using the same exploit kit actually continued.

Regarding new trends, from around mid-August Rig began to be observed. This is a comparatively new exploit kit that, like the previously-mentioned Angler and Nuclear, has functions for attacking vulnerabilities in Java, Flash, and Silverlight. It is provided as a paid service*43. In some of the cases in which Rig-based attacks were observed, redirection from a single redirection website to multiple exploit kits was seen.

Meanwhile, in many cases where the websites altered to redirect users were not well known, they stayed altered for two to four weeks at a time, and examples in which no investigation of the cause of alteration or fundamental countermeasures were carried out remain rife.

We estimate that drive-by download incidence as a proportion of the whole is in an upward trend. It is recommended that all parties affected 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.



*Covers several tens of thousands of sites in Japan. In recent years, drive-by downloads have been configured to change attack details and whether or not attacks are made based on the client system environment or session information, source address attributes, and the quota achievement status of factors such as number of attacks. This means that results can vary wildly at times depending on the test environment and circumstances.
*Because the Web crawler was not operating between July 1 and July 7, no attacks were detected during that period.

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

*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 See Malware don't need Coffee, "Angler EK : now capable of 'fileless' infection (memory malware)" (http://malware.dontneedcoffee.com/2014/08/angler-ek-now-capable-of-fileless.html) for more information about these functions.

*43 See Kahu Security, "RIG Exploit Pack" (http://www.kahusecurity.com/2014/rig-exploit-pack/) for more information about Rig.

1.4 Focused Research

Incidents occurring over the Internet change in type and scope from one minute to the next. Accordingly, IIJ works toward implementing countermeasures by continuing to perform independent surveys and analyses of prevalent incidents. Here we will present information from the surveys we have undertaken during this period regarding the Shellshock Bash vulnerability, as well as the POODLE attack. We will also cover the status of list-based attacks and their countermeasures.

1.4.1 The Shellshock Bash Vulnerability

About Shellshock

The CVE-2014-6271 vulnerability*44 was disclosed along with a fixed version of Bash*45 on September 24, 2014. This vulnerability could allow remote arbitrary code execution. Because Bash is a shell program that is normally used locally, people tend to think it is unaffected by remote attacks, but as the impact became clear there was a big uproar.

Although a fixed version was released at the same time that the vulnerability was disclosed, during the same week later several new related vulnerabilities were reported in quick succession. Table 1 shows a list of the related vulnerabilities. CVE-2014-7169*46 was registered as a new vulnerability because the original fix was deemed inadequate. CVE-2014-7186*47 and CVE-2014-7187*48 were vulnerabilities discovered during the process of making fixes. CVE-2014-6277*49 and CVE-2014-6278*50 were produced during the process of upstream maintainers merging the patches. To prevent attacks based on Shellshock, all these vulnerabilities must be patched.

Dealing with the Vulnerabilities

Because Bash is a shell program, unlike software such as server programs or scripting language interpreters, the functionality of the latest version is not often required. This means that the binary package provided for each distribution is used in most cases. Shellshock involves a number of vulnerabilities, but because some of these only affect fixes merged into upstream, the vulnerabilities that require action differ depending on the patches applied.

As an example for one distribution, Table 2 shows the status of each vulnerability in each release of CentOS*51. The version that fixes CVE-2014-6271 contains inadequate fixes just like the others, but subsequent vulnerabilities were fixed at the same time, and it is not affected by the CVE-2014-6277 and CVE-2014-6278 vulnerabilities that result from upstream fixes.

Table 1: List of Shellshock-Related Vulnerabilities

CVE ID	Date of Disclosure	Impact	Notes
CVE-2014-6271	September 24, 2014	Arbitrary code execution	The original vulnerability
CVE-2014-7169	September 25, 2014	Arbitrary code execution	Resulted from inadequate fixes to CVE-2014-6271
CVE-2014-7186	September 26, 2014	Arbitrary code execution	-
CVE-2014-7187	September 26, 2014	DoS	-
CVE-2014-6277	September 27, 2014	DoS	Resulted from upstream version fixes
CVE-2014-6278	September 27, 2014	Arbitrary code execution	Resulted from upstream version fixes

Table 2: Fixed Bash Packages for Each CentOS Release

CVE ID	CentOS 5	CentOS 6	CentOS 7
CVE-2014-6271	bash-3.2-33.el5.1	bash-4.1.2-15.el6_5.1	bash-4.2.45-5.el7_0.2
CVE-2014-7169	bash-3.2-33.el5_10.4	bash-4.1.2-15.el6_5.2	bash-4.2.45-5.el7_0.4
CVE-2014-7186			
CVE-2014-7187			
CVE-2014-6277	No fix necessary	No fix necessary	No fix necessary
CVE-2014-6278	No fix necessary	No fix necessary	No fix necessary

*44 CVE-2014-6271 bash: specially-crafted environment variables can be used to inject shell commands (https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2014-6271).
*45 GNU Bash: The GNU Bourne-Again SHell (http://www.gnu.org/software/bash/).
*46 CVE-2014-7169 bash: code execution via specially-crafted environment Incomplete fix for CVE-2014-6271 (https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2014-7169).
*47 CVE-2014-7186 bash: parser can allow out-of-bounds memory access while handling redir_stack (https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2014-7186).
*48 CVE-2014-7187 bash: off-by-one error in deeply nested flow control constructs (https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2014-7187).
*49 CVE-2014-6277 bash: uninitialized here document closing delimiter pointer use (https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2014-6277).
*50 CVE-2014-6278 bash: incorrect parsing of function definitions with nested command substitutions (https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2014-6278).
*51 CentOS Project (http://www.centos.org/).

This is because the Red Hat Enterprise Linux*52 that CentOS is based on dealt with the vulnerabilities by applying patches that fixed them to the base package rather than updating to the latest version of Bash. Whether or not other distributions are affected also depends on how fixes were applied.

The Impact of the Vulnerabilities

Let us examine why the vulnerabilities in Bash, which is used as a local shell, turned out to be exploitable remotely. These vulnerabilities apply when a Bash program is launched with specific environment variables set. In some environments Bash is run as the /bin/sh program used with shell-related calls, and these are also affected similarly.

Attacks that actually use these vulnerabilities have already been observed, with the most targeted area being CGI*53. To give an easily understandable example of the impact, there are some CGI programs written in Bash that run on Web servers, but these are almost never run on actual environments. However, even if a CGI program is written in another language, in some cases it is affected because it depends on the shell internally.

Linux is also often used as a control OS for appliance products or embedded devices. Some familiar examples are load balancers, home routers, and file servers. These may also have Bash embedded, or a management screen in which CGI is used, meaning that they are affected in the same way as normal Unix servers. In light of this, we will explain program execution in Unix environments, as well as the CGI processing flow, to show the impact of these vulnerabilities.

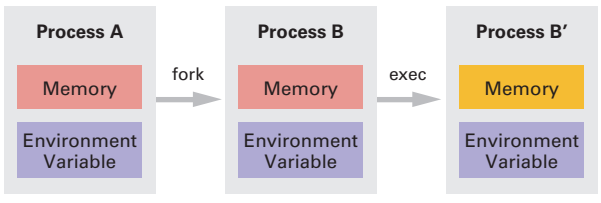
Program Execution in Unix Environments

Unlike Windows environments, in Unix environments it is not possible to create completely new processes. Instead, the procedure involves copying (forking) a parent process, and changing the child process into the process to execute (exec). Ultimately, the child process turns into the program to execute, becoming something different to the parent process. However, because it is copied, some of the data is carried over. Figure 13 shows the processing flow.

As shown in Table 3, there exist multiple varieties of exec functions called when making this change exist, and they differ in their handling of their handling of the environment variables that are the key factor for these vulnerabilities. For exec functions that do not explicitly specify an environment variable when called, the environment variables carried over from the parent process to the child process are still used after it changes into the process to execute.

CGI Processing Flow

CGI is a system for providing dynamic content via Web servers. It is less prevalent now that Web application frameworks have become more widespread, but it is still used. Web servers convert the headers received via HTTP into environment variables to launch the CGI program. This procedure is why CGI is the area most easily affected by these vulnerabilities. As long as Bash is not launched directly as a CGI program, it is not subject to the vulnerabilities at this point. However, as



- Process copied by forking
- Memory the same for Process A and B
- Environment variables also the same

- Changed to program to execute using exec
- Memory initialized
- Environment variables carried over as-is (except for execle and execve, which specifies environment variables explicitly)

Figure 13: Execution of External Programs in Unix Environments

Table 3: Operation of exec Functions

Function Name	Environment Variable Handling
execl	Carried over
execle	Explicitly specified
execlp	Carried over
execv	Carried over
execve	Explicitly specified
execvp	Carried over

*52 Red Hat Enterprise Linux (http://www.redhat.com/en/technologies/linux-platforms/enterprise-linux).
*53 RFC3875 The Common Gateway Interface Version 1.1 (http://www.ietf.org/rfc/rfc3875.txt).

mentioned earlier, the environment variables are carried over to the child process, so the vulnerabilities may apply if an external program is called via the shell, even if written in another language. In addition to directly-called programs, the same goes for programs called indirectly via libraries or modules. Figure 14 shows whether or not the vulnerabilities apply when programs are called via CGI.

With scripting language the shell may also be called unintentionally depending on how a program is written. Table 4 shows operation in Perl[*54] as an example of scripting language. As this demonstrates, even calls via the same function may be implicitly expanded to calls via the shell based on the parameters. Because all environment variables are carried over, when they are expanded to calls via the shell, the Shellshock vulnerabilities apply.

■ Summary

As explained above, even vulnerabilities in a program like Bash, which appears at first to be untouchable by remote attacks, may be attacked by external parties depending on how the program is used.

With these kinds of criteria for determining impact, it is difficult to comprehensively investigate all execution paths via a static inspection based on the source code. Meanwhile, unlike server programs, in many cases Bash updates do not require a reboot, so we recommend updating to a fixed version quickly if there is even the slightest suspicion that a system is affected.

Appliance products or embedded devices will require a firmware patch from the vendor. For some products it will take time before fixed firmware is released, and in this case provisional measures such as restricting access to areas suspected of being affected are also effective.

There are a range of techniques for dealing with vulnerabilities, such as applying workarounds, updating to a fixed version, or implementing protection using security devices. The best measure depends on the configuration of the system in question, so it is important to deal with the issue appropriately by evaluating each particular situation.

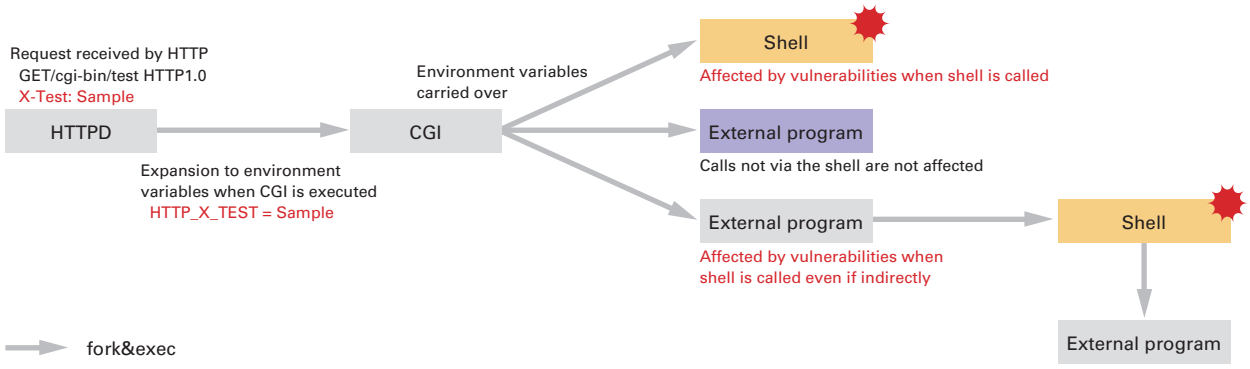


Figure 14: Impact on CGI

Table 4: External Program Calls in Perl

Perl Code	Expansion to exec Function	Shell Call	Environment Variables
`/bin/ls`	execvp("/bin/ls", ["/bin/ls"])	No	Carried over
`/bin/ls 2>/dev/null`	execl("/bin/sh", ["-c", "/bin/ls 2> /dev/null"])	Yes	Carried over
system("/bin/ls")	execvp("/bin/ls", ["/bin/ls"])	No	Carried over
system("/bin/ls &")	execl("/bin/sh", ["-c", "/bin/ls &"])	Yes	Carried over
open(FH, "/bin/ls |")	execvp("/bin/ls", ["/bin/ls"])	No	Carried over
open(FH, "/bin/ls 2>/dev/null |")	execl("/bin/sh", ["-c", "/bin/ls 2>/dev/null"])	Yes	Carried over

*54 The Perl Programming Language (https://www.perl.org/).

1.4.2 The POODLE Attack

On October 14, 2014 U.S. time, a new attack on SSLv3*55 was disclosed by Google's research team*56. This technique, known as the POODLE attack (Padding Oracle On Downgraded Legacy Encryption attack), is a MITM attack similar to the BEAST attack*57. It is used to decrypt target data encrypted with SSL one byte at a time through trial and error by sending large numbers of requests from a browser to a server. As far as practical damages go, it could result in the theft of cookies. Additionally, while it may appear at first as if this technique could also be applied to TLSv1.0*58, because of the differences in the padding methods used by SSLv3.0 and TLSv1.0, it is not practical as an attack on TLSv1.0. One the other hand, attacks can be made on SSLv3.0 by simply sending up to 255 queries to a server to sneak a glimpse of one byte. In this section, we examine the technical background of the POODLE attack, as well as its practicality*59.

■ An Overview of CBC Mode and its Potential Vulnerabilities

Like the BEAST attack, the POODLE attack only succeeds when CBC (Cipher Block Chaining mode) is used as the cipher mode. Stream cipher algorithms such as RC4 involve combining a keystream generated based on the key with plaintext using the XOR operation, enabling data of an arbitrary length to be encrypted. Meanwhile, block cipher algorithms such as DES or AES involve inputting data of a fixed length (the block length is 64 bits for DES and 128 bits for AES) into the cipher algorithm to obtain ciphertext of the same block length as the input length. When using block ciphers, the data to be encrypted is normally far larger than the block length, so it is necessary to encrypt many segments sequentially using the block cipher algorithm. The system that determines how the data obtained in the previous block cipher processing is used in the next data processing is called the cipher mode, and a number of systems have been proposed. Figure 15 shows an overview of one of these, the CBC cipher mode*60. First, an IV (Initial Vector)*61 of the block length is prepared as the initial value. Actual block cipher processing is carried out on data consisting of P_1, the first part of the plaintext after it is partitioned into block length segments, combined with the IV using the XOR operation. The output of this is the ciphertext C_1. To encrypt P_2, the second plaintext part, it is combined with C_1 obtained from the previous block cipher processing using the XOR operation, and this data is input as plaintext and encrypted, producing C_2 in a similar manner to before. In this way, encryption of the entire plaintext is calculated by repeating the cipher processing of $C_i = ENC(P_i \oplus C_{i-1})$. Conversely, for decryption the $P_i = DEC(C_i) \oplus C_{i-1}$ decryption processing is repeated sequentially to restore the plaintext.

For this cipher processing, when handling data that cannot be segmented at exactly block length, it becomes necessary to perform padding processing. This involves padding the last part of the plaintext with some form of data when it does not match the block length. Once padded to match the block length, block cipher processing can be carried out.

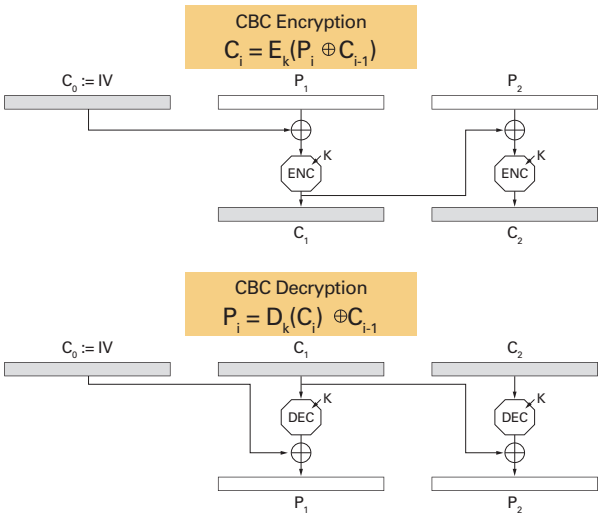


Figure 15: CBC Ciper Mode Overview

*55 IETF, "The SSL Protocol Version 3.0" (http://tools.ietf.org/html/rfc6101).

*56 Bodo Möller, Thai Duong, Krzysztof Kotowicz, "This POODLE Bites: Exploiting The SSL 3.0 Fallback" (https://www.openssl.org/~bodo/ssl-poodle.pdf).

*57 Thai Duong, Juliano Rizzo, "BEAST - Here Come The XOR Ninjas", 2011.

*58 IETF, "The TLS Protocol Version 1.0" (http://tools.ietf.org/html/rfc2246).

*59 This section places emphasis on the technical explanation. For an overview of the POODLE attack, see the following report from the Cryptographic protocol Evaluation toward Long-Lived Outstanding Security Consortium. On a new attack on SSLv3 specification called POODLE attack (https://www.cellos-consortium.org/index.php?PoodleAttack_20141015).

*60 NIST, "NIST Special Publication 800-38A Recommendation for Block Cipher Modes of Operation: Methods and Techniques" (http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf).

*61 The IV (Initial Vector) does not need to be kept secret. However, as with a key, the IV is required at the time of decryption.

TLS uses the PKCS#5 padding scheme*62, and Figure 16 shows an example of padding when the block length is 8 bytes (for example DES). Because case (a) is 3 bytes short of the block length, that 3 byte space is filled with 0x03 as padding data. In the same way, case (b) is 5 bytes short so that 5 byte space is filled with 0x05. Although (c) is a case in which the data to be encrypted is a multiple of the block length, to identify the boundary showing how much padding was added to the plaintext, it is treated as 8 bytes short (exactly the block length), and this block is completely filled with 0x08.

Meanwhile, SSLv3.0 uses a different padding scheme, and this difference is one of the factors that brought about the POODLE attack. Figure 17 shows the differences between PKCS#5 padding and SSLv3 padding. The padding scheme used with SSLv3 assigns the padded byte length to the final byte when padding, just as with PKCS#5 padding. Random data is used for the rest of the padding data. Unfortunately, for both SSLv3 and TLS this padded area does not fall within the scope of the MAC (Message Authentication Code) data that indicates data has not been altered over the communication channel. That means even if the padding data is altered, these alterations cannot be detected via MAC verification. On one hand, while with TLS the constraints of the padding data explained above may enable alterations to the padded part to be detected, with SSLv3 there is no way to detect alterations to the padding data other than the final byte. You could say that the POODLE attack targets this tiny gap in the protocol's armor.

Figure 18 shows the extent of impact for decryption using CBC mode when the ciphertext has been altered. In this figure, the entire P_1 plaintext block has been changed by altering part of the C_1 ciphertext. However, the attacker is able to freely change the intended area of the P_2 plaintext. Figure 19 shows the principles of padding oracle attacks*63 that exploit this characteristic. Assuming that the plaintext length is known, and data up to P_n is encrypted, the man-in-the-middle replaces the last block C_n with the attack target, or in others words the C_i data they want to decrypt. Because the plaintext length is already known at this time, the last byte of P_n that stores the padded data length is also known. SSL/TLS servers conduct

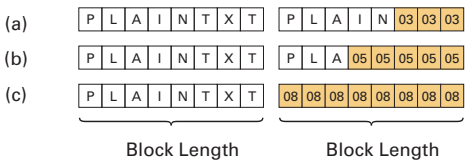
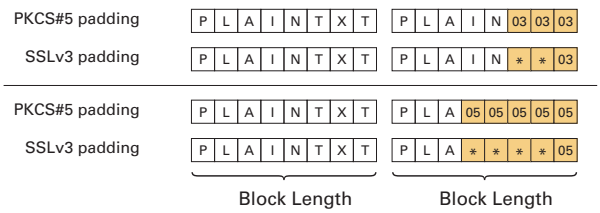
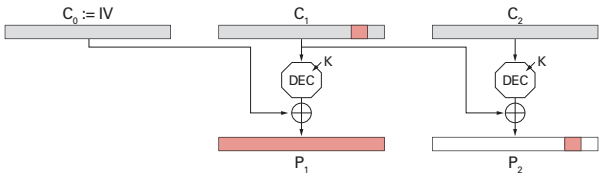


Figure 16: PKCS#5 Padding Example with Block Length of 8 Bytes



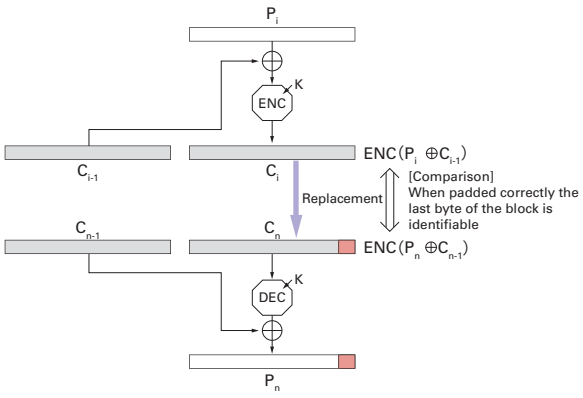
The "" marks in colored padding data indicate random data.

Figure 17: Differences Between PKCS#5 Padding Scheme and SSLv3 Padding Scheme



*When a single byte of the ciphertext is altered and decrypted, this affects the entire block of the plaintext for the corresponding block, but it allows the intended area of the plaintext for the next block to be altered.

Figure 18: Extent of Impact When Ciphertext is Altered in CBC Mode



*The server's padding check function accepts data when padding is correct, but returns an error when it is incorrect.

Figure 19: Padding Oracle Attack Principles

*62 IETF, "PKCS #5: Password-Based Cryptography Specification Version 2.0" (http://tools.ietf.org/html/rfc2898).

*63 In addition to SSL/TLS, the same kind of attack has been disclosed for SSH and IPsec. In both cases, these attack methods decipher encrypted data by determining whether it conforms to data format constraints determined by the specifications based on error information from the server. M.R. Albrecht, K.G. Paterson, G.J. Watson, Plaintext Recovery Attacks Against SSH, 30th IEEE Symposium on Security and Privacy, 2009. (http://www.isg.rhul.ac.uk/~kp/SandPfinal.pdf). J.P. Degabriele and K.G. Paterson, On the (In)security of IPsec in MAC-then-Encrypt Configurations, Proceedings of the 17th ACM Conference on Computer and Communications Security, 2010. (http://portal.acm.org/citation.cfm?id=1866363).

a padding check according to procedure, and an error is returned if the data does not conform to the padding scheme determined by the specifications. Using this error return function (padding oracle) means that when the server accepts the encrypted data, the correct data is stored in the padded part. In SSLv3, the data is accepted if the last byte of P_i and P_n match. As a result, it is possible to decrypt the last byte of P_i (even when the encryption key is not known) because the last byte of $P_i \oplus C_{i-1}$ and $P_n \oplus C_{n-1}$ match. In actual fact, because a MAC-based check is implemented, it is possible to detect whether the plaintext part before the padding data has been altered, so in most cases this doesn't work. However, as pointed out with the POODLE attack, when that block is somehow filled solely with padding data (as with (c) in Figure 16), the final block can be removed from the scope of MAC verification. When testing whether the last byte matches, it will definitely be accepted once every 256 times. Meanwhile, for TLS all bytes in the block must be filled with the same data, as shown in (c) of Figure 16. In this example the block length is 8 bytes, so just one in every 2^{64} attempts will be successful. For AES the block length is 16 bytes, making 2^{128} attempts necessary, meaning for TLS this attack is regarded as a potential problem that is not currently practical. However, the POODLE attack identified here only requires around 2^8 calculations to decrypt 1 byte, so it is recognized as a practical attack.

■ The Practicality of the POODLE attack

For SSH, the CTR cipher mode was available in addition to the CBC mode, so by shelving the use of CBC mode it was possible to prevent padding oracle attacks. However, for SSL/TLS the use of CTR mode is not established in the specifications. Additionally, for the CipherSuites (cryptographic algorithms) specified in the SSLv3 specifications, other than algorithms with only 40-bit key strength that were formerly used for export controls, or NULL (no encryption), the only option available when CBC mode is not used is RC4. However, last year new methods for attacking RC4 were disclosed in quick succession*64*65, and it is now seen as a vulnerable algorithm.

The BEAST attack is classified as a padding oracle attack like the POODLE attack, and can be made successfully on SSLv3 and TLSv1.0. The TLSv1.1 specification is designed to work around this vulnerability. More specifically, it avoids the underlying problem of cipher data from the previous session being used as the IV for the next session by implementing a process that generates a new IV. SSLv3 and TLSv1.0 are still in use despite the BEAST attack existing because the technique called 1/n-1 splitting is known to be an effective countermeasure*66. This technique has already been implemented in major browsers, but it cannot be applied to POODLE attacks. It is possible that techniques like 1/n-1 splitting for prolonging the life of SSLv3 will be devised in the future. However, at this point in time there is no longer any way to use SSLv3 safely.

There are two fundamental countermeasures for this attack: 1) disable SSLv3 (on either the client or server), or 2) implement TLS_FALLBACK_SCSV (both client and server must support it). With regard to the first approach, major browsers have announced they will disable SSLv3 in the future*67*68*69. Additionally, instructions for disabling SSLv3 in browsers yourself have been made available*70*71. Methods for disabling SSLv3 on the server side are also being shared*72. Meanwhile, we believe it will be difficult to implement measures for legacy products such as feature phones and game devices. For that reason, once SSL/TLS servers remove support for SSLv3, in some cases it will no longer be possible to view sites on these devices.

*64 Takanori ISOBE, Toshihiro OHIGASHI, Yuhei WATANABE, and Masakatu MORII, "Full Plaintext Recovery Attack on Broadcast RC4,", Proc. the 20th International Workshop on Fast Software Encryption (FSE 2013), 2013. (Revised Selected Papers, LNCS 8424, pp.179-202, Springer-Verlag, 2014).

*65 N.AlFardan, D.J.Bernstein, K.G.Paterson, B.Poettering, J.C.Schuldt, On the Security of RC4 in TLS, USENIX Security 2013. (http://dl.acm.org/citation.cfm?id=2534793).

*66 ImperialViolet, "POODLE attacks on SSLv3 (14 Oct 2014)" (https://www.imperialviolet.org/2014/10/14/poodle.html).

*67 Mozilla Security Blog, "The POODLE Attack and the End of SSL 3.0" (https://blog.mozilla.org/security/2014/10/14/the-poodle-attack-and-the-end-of-ssl-3-0/). *68 Google Online Security Blog, "This POODLE bites: exploiting the SSL 3.0 fallback" (http://googleonlinesecurity.blogspot.jp/2014/10/this-poodle-bites-exploiting-ssl-30.html).

*69 "Microsoft Security Advisory 3009008, Vulnerability in SSL 3.0 Could Allow Information Disclosure" (https://technet.microsoft.com/en-us/library/security/3009008).

*70 SANS ISC InfoSec Handlers Diary Blog, "OpenSSL: SSLv3 POODLE Vulnerability Official Release" (https://isc.sans.edu/diary/OpenSSL%3A+SSLv3+POODLE+Vulnerability+Official+Release/18827).

71 mozillaZine, "Security.tls.version." (http://kb.mozillazine.org/Security.tls.version.*).

*72 F5 Networks, "CVE-2014-3566: Removing SSLv3 from BIG-IP" (https://devcentral.f5.com/articles/cve-2014-3566-removing-sslv3-from-big-ip).

The second countermeasure is a method proposed for fundamentally protecting against downgrade attacks*73*74. For this method the TLS_FALLBACK_SCSV CipherSuite value and inappropriate_fallback error code are added, making it possible to protect against downgrade attacks as long as both the client and server support this SCSV (Signaling Cipher Suite Value)*75. Its behavior is extremely simple, with a client including this SCSV in the CipherSuites of the ClientHello message when it connects to a server using a protocol other than the highest version it supports. Meanwhile, a server receiving a CipherSuites with this SCSV returns an error if the protocol version specified by the client is lower than the highest version supported by the server. Through this behavior, it is possible to avoid potential downgrade attacks. Currently the draft is at last call status in the TLS WG, but SCSV has been implemented on Google servers and in Chrome (version 33 or later) since February of this year. The version of OpenSSL released on October 15 also implements SCSV. Support is planned for Firefox*76, and in the future we expect use of SCSV on servers and clients will continue to gather momentum. However, until both servers and clients support this countermeasure, it will not be possible to prevent the POODLE attack. It is very unlikely that these countermeasures will be widely applied in legacy environments such as feature phones, so you could regard these as being implemented to guard against potential attacks in the future.

Because generating a large volume of requests from a browser and rewriting some of them over the communication path (to replace the targeted cipher data) are prerequisites of the POODLE attack, in a similar manner to the BEAST attack it is not necessarily possible to easily launch attacks with typical usage environments. However, in this case the issue is with the protocol specification itself, and due to the difficulty of implementing workarounds, SSLv3 is seen as vulnerable like SSLv2, so we do not believe it is wise to continue using it in the future. In fact, Twitter and a number of other services announced they would disable SSLv3 right away*77*78.

In addition to the TLSv1.0 TLS specification, TLSv1.1 and TLSv1.2 have also been standardized and are widely implemented. The former fixes the BEAST attack, and the latter features the more secure SHA-256 and SHA-384 hash functions, as well as support for GCM and CCM cipher modes besides CBC. Furthermore, TLSv1.3*79 is currently under discussion in the TLS WG. The elimination of CBC as a cipher mode is being looked into, and preparation for enabling secure use through using the latest protocol version is well underway. Just as the use of cryptographic algorithms such as DES and MD5, which were formerly considered secure and widely used, ceased when they were compromised*80, it will also be necessary to discard past versions of cryptographic protocols and swiftly migrate to new versions. In doing so, we will need to weigh the balance between backward compatibility (the ratio of SSL clients that will no longer be able to connect after moving to a newer version) and security (the urgency of implementing countermeasures).

*73 MITM attacks that involve intentionally forcing the server and client to use an older protocol version. The ClientHello contains a space for specifying the version that the client supports, and by specifying SSLv2 here it is possible to force the use of an weaker algorithm involuntarily. In SSLv2 there is no fundamental solution for downgrade attacks because this message is not protected by MAC, so SSLv2 is recognized as a vulnerable version.

*74 IETF, "TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks" (https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv). The draft that was initially a personal proposal (https://tools.ietf.org/html/draft-bmoeller-tls-downgrade-scsv-02) is now taken up for discussion in the TLS WG.

*75 Originally, the CipherSuite was 2-byte data that indicated the class of cryptographic algorithm used in SSL/TLS. However, as with the TLS_EMPTY_RENEGOTIATION_INFO_SCSV value introduced in RFC5746 (http://tools.ietf.org/html/rfc5746) to deal with the renegotiation function problem discovered in 2009, it has been expanded to serve different purposes than originally intended.

*76 http://www.ietf.org/mail-archive/web/tls/current/msg13905.html

*77 https://twitter.com/twittersecurity/status/522190947782643712

*78 CloudFlare blog, "SSLv3 Support Disabled By Default Due to POODLE Vulnerability" (https://blog.cloudflare.com/sslv3-support-disabled-by-default-due-to-vulnerability/).

*79 The Transport Layer Security (TLS) Protocol Version 1.3 (https://tools.ietf.org/html/draft-ietf-tls-tls13). See https://github.com/tlswg/tls13-spec for discussion of this version.

*80 Examples of the compromise of cryptographic algorithms are provided in Vol.8 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol08_EN.pdf) under "1.4.1 Trends in the Year 2010 Issues on Cryptographic Algorithms".

1.4.3 The Status of List-Based Attacks and Their Countermeasures

About List-Based Attacks

Since last year there has been a spate of incidents of unauthorized access on a range of online services using attack methods known as list-based attacks and list-based account hackings. List-based attacks are those that involve attackers making ongoing attempts to log in to a service using a list of login ID and password pairs. The lists used in attacks are created from information leaked from services other than the attack target. Attackers use these lists in attacks because many users reuse that same login ID and password on multiple services*81.

When an attacker logs in successfully, from the service provider's perspective it is difficult to determine whether or not they are a legitimate user, and this enables the attacker to achieve their purpose before measures are taken. The more services that a user reuses the same login ID and password on, the greater the extent of damages to them could be.

Differences Compared to Other Login Attempt Attacks

Some well known examples of login attempt attack methods that target specific login IDs include brute-force attacks, which attempt to use a variety of passwords sequentially, and dictionary attacks, which attempt to use words and phrases commonly used as passwords. List-based attacks are different in that the login ID and password pairs used in attempts are already determined in advance.

The Status of List-Based Attacks in 2014

Table 5 summarizes the incidents reported as list-based attacks that occurred between January 1 and September 30, 2014. This shows that practically every month services have been targeted by list-based attacks, resulting in unauthorized logins. There were also nine incidents that resulted in financial damages, including cases in which a credit card was used to purchase large numbers of tickets, which were then converted to cash, as well as cases in which messages impersonating a friend were sent to request victims to buy prepaid cards. In addition to these, there were incidents in which service points were converted into gift vouchers without authorization. In 13 cases the list-based attack was discovered by the service provider, while in 9 cases it was the user that discovered the attack. This demonstrates that in many cases the service provider is not aware that a list-based attack has taken place.

List-Based Attack Countermeasures on Online Services

Last of all, we explain the list-based attack countermeasures that can be implemented by service providers and users below*82. However, these countermeasures are based on the provision/use of a service, and some areas may not be applicable to internal systems.

List-Based Attack Countermeasures for Service Providers

The three main countermeasures for service providers are (1) improvements to the design and implementation of authentication functions, (2) improvements to system monitoring and operation, and (3) providing monitoring and notification functions for user activity. Additionally, when making countermeasures, it is necessary to implement them without placing undue burden on users.

The countermeasures under (1) involve improving login ID and password settings, and providing authentication other than passwords. To prevent the same login ID and password being reused, consider auto-generating login IDs and passwords based on system policy. This makes it possible to prevent the reuse of login IDs and passwords from other services*83. When allowing users to set their own passwords, it is necessary to reject weak passwords*84 and make it clear that login IDs and passwords should not be reused.

In addition, you must look into supplementing this with multi-step authentication or multifactor authentication (hardware tokens or IC cards) on the assumption that some users will still reuse passwords from elsewhere. To implement these the system will need to be modified in some cases.

---

*81 The "Stop reusing passwords! A call to prevent unauthorized login due to password list attacks" (https://www.jpcert.or.jp/pr/2014/pr140004.html) (in Japanese) article published by the IPA and JPCERT/CC states that approximately a quarter (25.4%) of users use the same password at money-related service sites.

*82 The Ministry of Internal Affairs and Communications also published "Measures for dealing with unauthorized logins due to list-based account hacking" (http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000063.html) (in Japanese) for service providers.

*83 Because it is technically difficult to prevent users from using the login IDs and passwords generated by a service provider on another service, it is necessary to warn users not to use the same details on other services.

*84 It is necessary to prevent users from setting weak passwords that are easy to guess, such as "password," "123456," the user's name, address, or birthday, or a combination of these.

It is also not possible to say with any certainty that information will not leak from your own system due to vulnerabilities, etc. That means it is necessary to take measures to prevent attackers from using authentication information in list-based attacks once they obtain it, in the event that login IDs or passwords leak from your own service. When saving passwords, instead of saving as plain text or using simple hashing, use hash based password stretching with salt to make it impossible to analyze in a practical amount of time. When you cannot implement this yourself, you can also use authentication functions provided by external organizations. However, you must also take into consideration the risk of outsourced authentication systems being attacked.

The countermeasures under (2) apply before and after an attack occurs. When a list-based attack is carried out, in some cases you will observe symptoms not normally seen, such as a higher load on the system, a larger number of failed login attempts, many login attempts being made with login IDs that do not exist, an abnormal number of login attempts from a specific IP address using different login IDs each time, and access from an IP address block not normally seen.

Look at implementing a system that can notify administrators, automatically block attackers' IP addresses, and lock accounts when symptoms such as these are detected*85. Additionally, deleting accounts that have not been used in a long time can prevent damages caused by list-based attacks before they happen.

Table 5: List-Based Attack Incidents in 2014

Disclosure Date	Service Type	Service Provider	Period	Unauthorized Login Attempts	Successful Unauthorized Logins	Discovered By	Financial Damages	Main Countermeasures
Jan. 24	Communications-related service	Company A	Jan. 16	Not known	165	Not known	None	(1) (2) (3) (5) (13)
Feb. 24	Blog service	Company B	Not known	Not known	Not known	Service provider	Unauthorized point conversion	(6) (16)
Feb. 25	SNS	Company C	Feb. 5 to Feb. 11	Not known	370	User	None	(1) (6)
Feb. 28	SNS	Company C	Feb. 28	Not known	16,972	Not known	None	(1) (5) (7) (13) (18)
Feb. 28	Communications-related service	Company D	Feb. 24 to Feb. 25	Approx. 15,000	344	Service provider	Unauthorized content purchase	(2) (3) (4) (5) (7) (10) (13)
Mar. 16	Point-related service	Company E	Mar. 16 to Mar. 17	Approx. 940,000	Approx. 19,000	Service provider	None	(4) (5) (7) (9) (13)
Apr. 23	Member site	Company F	Mar. 23 to Apr. 21	4,600,000	78,361	Service provider	None	(3) (5) (7) (8) (9) (13) (14)
Apr. 30	Communications-related service	Company D	Apr. 14 to Apr. 28	Not known	724	Service provider	Unauthorized content purchase	(2) (3) (4) (5) (7) (10) (13)
May 2	Point-related service	Company G	Apr. 19 to Apr. 29	Not known	273	User	Unauthorized point conversion	(2) (4) (7) (9)
May 30	E-commerce service	Company H	Sept. 2013 to Mar. 2014	Not known	Not known	Not known	Unauthorized content purchase	(19)
June 10	Video service	Company I	May 27 to June 4	2,203,590	219,926	User	Unauthorized point conversion	(13) (17)
June 12	SNS	Company J	Not known	Not known	303	User	Prepaid card purchase	(3) (6)
June 17	SNS	Company C	May 30 to June 17	Approx. 4,300,000	263,596	User	None	(1) (3) (6) (13) (15)
June 20	Blog service	Company B	June 16 to June 19	Approx. 1,600,000	2,398	User	None	(12) (13)
June 23	Blog service	Company K	June 19 to June 23	2,293,543	38,280	Service provider	None	(13)
June 26	Survey service	Company L	June 23 to June 24	Not known	Up to 11,502	User	Unauthorized point conversion	(1) (3) (17)
June 30	Game related	Company M	June 28 to June 29	1,796,629	14,399	Service provider	None	(3) (14)
July 1	Ad service	Company N	Irregularly since Aug. 2013	Not known	Not known	Not known	Not known	(7)
July 4	Survey service	Company O	June 25	3,420,000	15,092	Service provider	Unauthorized point conversion	(3) (5) (13)
July 4	Game related	Company P	Not known	Not known	Not known	User	Not known	(5) (8)
Aug. 13	E-commerce service	Company Q	Aug. 7 to Aug. 12	4,220,382	20,957	Not known	None	(13)
Aug. 18	Point-related service	Company E	Aug. 15	Approx. 296,000	756	Service provider	None	(13)
Aug. 27	Game related	Company P	Not known	Not known	Not known	User	Not known	(5) (8) (11)
Sept. 11	Logistics service	Company R	Sept. 10 to Sept. 11	Approx. 11,520,000	Approx. 21,000	Service provider	None	(5) (7) (8) (9) (13)
Sept. 23	E-commerce service	Company Q	Sept. 22 to Sept. 23	18,663	19	Not known	None	(13)
Sept. 26	Logistics service	Company S	Sept. 25 to Sept. 26	Approx. 190,000	10,589	Service provider	None	(1) (5) (7) (8) (9) (13)
Sept. 29	Logistics service	Company T	Not known	Not known	34,161	Service provider	None	(1) (5) (7) (8) (9) (13)
Sept. 30	Communications-related service	Company U	Sept. 27 to Sept. 29	Approx. 2,250,000	6,072	Service provider	None	(1) (5) (7) (8) (9) (11) (14)

(1) Block attacker's IP address
(2) Bolster detection system
(3) Bolster authentication function
(4) Bolster monitoring system
(5) Notify all users that reuse of passwords is prohibited
(6) Request that all users change their passwords
(7) Request that all users change password regularly
(8) Notify all users that previously used passwords are prohibited
(9) Notify all users that easy to guess passwords are prohibited
(10) Notify all users to be wary of phishing sites
(11) Notify all users that two-step authentication is recommended
(12) Force users logged in without authorization to log out
(13) Reset passwords of users logged in without authorization or request them to change their passwords
(14) Lock the account of users logged in without authorization
(15) Lock dormant accounts
(16) Modify system
(17) Shut down part of system
(18) Delete malicious posts
(19) Assist police with investigation

*85 Symptoms such as these reflect current attack trends, and in the future these patterns may change. It is necessary to gather information on the latest attack trends, and perform monitoring with these in mind. Additionally, regarding the legal issues surrounding the privacy of communications, such as the identification of symptoms and automatic blocking based on this, see "Section 4: Dealing with spam that exploits SMTP authentication information" in the "Initial Report of the Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business" (http://www.soumu.go.jp/main_content/000283608.pdf) (in Japanese), and "(4) Dealing with spam that exploits SMTP authentication information" in the "Guidelines for Dealing with High Volume Communications and Privacy at Telecommunications Carriers" (http://www.jaipa.or.jp/other/mtcs/guideline_v3.pdf) (in Japanese).

When an unauthorized login is detected, consider shutting down the service to prevent the spread of damage and investigate the matter. The password for the account that was logged into without authorization must be changed to prevent further unauthorized login, such as by resetting it. To be on the safe side, also look into changing the passwords for accounts that were not subject to unauthorized login as well.

The countermeasures under (3) are functions for alerting users when important processes are carried out. At times such as when login succeeds or fails, when personal information is viewed or changed, or when purchase settlement processing is complete, notifying users by email will enable them to realize when unauthorized access has occurred. Additionally, providing functions that enable login history or purchase history to be viewed makes it possible to identify the approximate time that unauthorized access takes place.

List-Based Attack Countermeasures for Users

When users set their password themselves, the most effective way to do it is by using password management software to generate and manage different passwords for each service. For web-based services, there is also the method of having the web browser remember passwords created with a password generation tool*86. However, to cope with the risks that arise from using Web browsers, always set a master password*87, and use the latest version of the Web browser.

When a service provides two-step authentication, always endeavor to use it. Also enable notifications in the service, and when a notification showing usage you have no knowledge of arrives, change the password as soon as possible, check that no financial damages have been incurred, and contact the service administrator. It is also a good idea to delete your account when you don't intend to use a service anymore.

1.5 Conclusion

This report has provided a summary of security incidents to which IIJ has responded. In this volume we examined the Shellshock Bash vulnerability, and discussed the POODLE attack. We also summarized the current status and countermeasures for list-based attacks. IIJ makes every effort to inform the public about the dangers of Internet usage by identifying and publicizing incidents and associated responses in reports such as this. IIJ will continue striving to provide the necessary countermeasures to allow the safe and secure use of the Internet.

Authors:

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

Hirohide Tsuchiya (1.2 Incident Summary)
Hirohide Tsuchiya, Tadaaki Nagao, Hiroshi Suzuki, Hisao Nashiwa (1.3 Incident Survey)
Tadashi Kobayashi (1.4.1 The Shellshock Bash Vulnerability)
Yuji Suga (1.4.2 The POODLE Attack)
Minoru Kobayashi (1.4.3 The Status of List-Based Attacks and Their Countermeasures)
Office of Emergency Response and Clearinghouse for Security Information, Service Operation Division, IIJ

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

*86 When managing passwords using a Web browser, there is a chance that passwords will be stolen if the computer is infected with malware, but this can be thought of as one practical method of managing a large number of complicated passwords using a familiar tool.

*87 A master password can be set in Firefox. In other major Web browsers (Internet Explorer, Google Chrome, Safari), passwords are automatically encrypted and saved using the security mechanisms of the OS, etc.