Home Router Security

In this report, we discuss detection of the ZeroAccess malware, and examine the state of home router security as well as various associated risks. We also look at the spate of unauthorized login incidents that have occurred since the beginning of this year.

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 April 1 through June 30, 2013. Continuing on from the last survey period, a number of hacktivism-based attacks were made by Anonymous and other groups. There were also a series of Web server compromises and related website alterations. In April there were many incidents of unauthorized access to portal sites and shopping sites. In a number of cases, it is speculated these were attempts to commit fraud using a list of IDs and passwords thought to have been obtained from other websites. Multiple attacks on domain registries including ccTLD continue to occur, along with associated domain hijackings and information leaks. As seen above, the Internet continues to experience many security-related incidents.

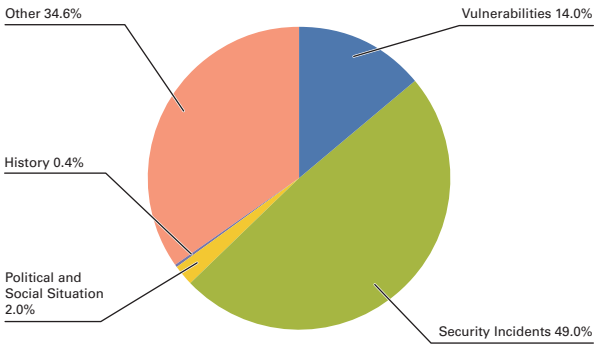


Figure 1: Incident Ratio by Category (April 1 to June 30, 2013)

1.2 Incident Summary

Here, we discuss the IIJ handling and response to incidents that occurred between April 1 and June 30, 2013. Figure 1 shows the distribution of incidents handled during this period*1.

■ The Activities of Anonymous and Other Hacktivists

Attacks by hacktivists such as Anonymous continued during this period. DDoS attacks and information leaks occurred at government-related and company sites in a large number of countries stemming from a variety of incidents and causes. High-profile incidents included a series of attacks on websites related to the government of North Korea, in which a number of websites were altered and account information leaked (OpNorthKorea). There were also a number of attacks on Israeli government and related sites (OpIsrael), as well as attacks from the Israeli side thought to have been carried out in retribution. A number of people have been arrested in Jordan on suspicion of being involved in these attacks. DDoS attacks were also made on websites of government institutions and media outlets in Turkey to protest a police crackdown on demonstrations against public-works projects (OpTurkey). Over 30 suspects have been arrested by Turkish authorities in connection with these attacks as well. Retaliation continues in both cases, including further attacks carried out in protest against the arrest of suspects. In

*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.

attacks targeting U.S. government agencies and financial institutions in May (OpUSA), several hundred websites experienced alterations, information leaks, or DDoS attacks, but the impact was limited*2. In June, attacks were made on international petroleum gas companies and oil-producing nations (OpPetrol), but these were also not large in scale.

Groups other than Anonymous continue to be very active.

■ Vulnerabilities and their Handling

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

Regarding server applications, a quarterly update for the Oracle database server was released, fixing many vulnerabilities. A vulnerability in BIND9 DNS server that caused abnormal server stoppages through processing requests to certain resource codes was also fixed*9.

A vulnerability with no fix available resulting from improper PHP settings in a version of the Parallels Plesk Panel server management tool for which support had ended was disclosed. Due to reports that this vulnerability could be easily exploited*10, users were urged to upgrade to the latest supported version. A number of vulnerabilities were also discovered and fixed in the Apache Struts Web application framework. Multiple vulnerabilities in WordPress, including those involving elevation of privileges and cross-site scripting, were also fixed.

■ Increasing Prevalence of Compromised Web Servers

During this survey period, Web server compromises and related website alterations attracted a lot of attention. Many of the altered websites had iframe elements or obfuscated JavaScript that redirected users to other websites embedded in them. These caused users to be taken to malicious websites after viewing an altered website, possibly infecting them with malware. The malicious websites that users were redirected to had exploit kits such as BHEK2 (Blackhole Exploit Kit Version 2) installed, so this activity is thought to have been coordinated. A number of websites were altered, including those for companies and organizations. An alert from the JPCERT Coordination Center*11 indicated that at the time of its issue approximately 1,000 incidents have been reported since April of this year.

Many vulnerabilities in old versions of CMS (Content Management System) and server management tools, including those for which support had ended, had been targeted on the altered websites*12. For this reason, an alert was issued regarding several vulnerabilities thought to be particularly dangerous*13.

---

*2 See the following Trend Micro SECURITY INTELLIGENCE BLOG post for details regarding these attacks. "Failed OpUSA Attacks Show How Hackers Operate" (http://blog.trendmicro.com/trendlabs-security-intelligence/failed-opusa-attacks-show-how-hackers-operate/).

*3 Microsoft, "Microsoft Security Bulletin MS13-029 - Critical: Vulnerability in Remote Desktop Client Could Allow Remote Code Execution (2828223)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-029).

*4 "Microsoft Security Bulletin MS13-028 - Critical: Cumulative Security Update for Internet Explorer (2817183)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-028).

*5 "Microsoft Security Bulletin MS13-037 - Critical: Cumulative Security Update for Internet Explorer (2829530)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-037).

*6 "Microsoft Security Bulletin MS13-038 - Critical: Security Update for Internet Explorer (2847204)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-038).

*7 "Microsoft Security Bulletin MS13-047 - Critical: Cumulative Security Update for Internet Explorer (2838727)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-047).

*8 "Microsoft Security Bulletin MS13-051 - Important: Vulnerability in Microsoft Office Could Allow Remote Code Execution (2839571)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-051).

*9 The JPCERT Coordination Center issued an alert regarding this vulnerability. "JPCERT/CC Alert 2013-06-05 Denial of service vulnerability in ISC BIND 9 (CVE-2013-3919)" (http://www.jpcert.or.jp/english/at/2013/at130026.html).

*10 See the following Cisco Blogs post for details regarding this vulnerability. "Plesk 0-Day Targets Web Servers" (http://blogs.cisco.com/security/plesk-0-day-targets-web-servers/).

*11 JPCERT Coordination Center, "JPCERT/CC Alert 2013-06-07 Alert regarding compromised websites" (http://www.jpcert.or.jp/english/at/2013/at130027.html).

*12 For example, in June the Information-technology Promotion Agency, Japan published "Reminder for this Month - Implement measures to prevent your website from being compromised!" (http://www.ipa.go.jp/security/txt/2013/06outline.html) (in Japanese), which indicated that these were the source of most of the web alterations reported to IPA.

*13 JPCERT/CC, "JPCERT/CC Alert 2013-04-08 Alert regarding the usage of old versions of Parallels Plesk Panel" (http://www.jpcert.or.jp/english/at/2013/at130018.html).

April Incidents

1 **1st:** Trouble occurred at 200 local authorities around Japan, rendering the Basic Resident Register Network inaccessible. This was caused by data verification work related to a failure that occurred in March dragging on longer than expected.

2 **2nd:** Attempts were made to log in to gooIDs without authorization, and accounts were locked due to the possibility of unauthorized login to 108,716 accounts. There was evidence that a list of IDs and passwords that had leaked from a competitors' service had been used in attempts to log in to the gooID system.
NTT Resonant Inc., "Regarding the impact caused by unauthorized login to gooIDs" (final report) (http://pr.goo.ne.jp/detail/1703/) (in Japanese).

3

4 **4th:** Fraudulent attempts were made to log in to the FLET'S Hikari member's site, and it was discovered that 30 accounts may have been logged into without authorization. As a result, restrictions were placed upon accounts and login to the site.
Nippon Telegraph and Telephone East Corporation, "Regarding Unauthorized Access to the FLET'S Hikari Members Club" (http://www.ntt-east.co.jp/release/detail/20130404_02.html) (in Japanese).

5 **5th:** Between April 1 and April 5, 2013, unauthorized logins took place at a site that sells electronic books. Passwords were reset for user IDs corresponding to 779 accounts that were logged into from IP addresses suspected to be malicious.

6 **5th:** It was announced that fraudulent activity had occurred on March 26 through unauthorized login to a membership rewards points site, resulting in reward points for 299 IDs being used.

7 **5th:** The Information Security Advisory Board of the Ministry of Internal Affairs and Communications officially announced its "Proposals on Promotion of Information Security Policy of MIC." This summarized advice from a range of perspectives regarding the direction for measures that should be taken regarding the promotion of information security in the short and long term, as well as improvements to existing initiatives.
"Official Announcement of Proposals on Promotion of Information Security Policy of MIC" (http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/130405_02.html).

8 **6th:** WordPress.com announced support for an optional Two Step Authentication feature using Google's authentication system.
Just Another WordPress Weblog, "Greater Security with Two Step Authentication" (http://en.blog.wordpress.com/2013/04/05/two-step-authentication/).

9 **8th:** The JPCERT Coordination Center issued an alert due to the prevalence of old versions of Parallels Plesk Panel being used in incidents of Web alterations involving the installation of malicious Apache modules.
"JPCERT/CC Alert 2013-04-08 Alert regarding the usage of old versions of Parallels Plesk Panel" (http://www.jpcert.or.jp/english/at/2013/at130018.html).

10 **10th:** Microsoft published their Security Bulletin Summary for April 2013, and released two critical updates including MS13-028 and MS13-029, as well as seven important ones including MS13-035.
"Microsoft Security Bulletin Summary for April 2013" (http://technet.microsoft.com/en-us/security/bulletin/ms13-Apr).

11 **10th:** A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB13-11: Security updates available for Adobe Flash Player" (http://www.adobe.com/support/security/bulletins/apsb13-11.html).

12 **10th:** With the establishment of systems such as CSIRT at government ministries, the 1st PoC (Point of Contact) assembly was held, consisting of the CSIRT representative (PoC) from each government ministry.
National Information Security Center, "Regarding Convening of the 1st Government Ministry PoC Assembly" (http://www.nisc.go.jp/press/pdf/01poc.pdf) (in Japanese).

13

14 **11th:** Fraudulent websites for a number of financial institutions were discovered, generating a lot of interest. It was pointed out that these may be conversion services for mobile communications.
For example, the following statement was made from the JPCERT Coordination Center Twitter account (https://twitter.com/jpcert/status/322282948554530816) (in Japanese).

15 **12th:** In relation to the Remote Control Virus incident, it was reported that journalists from news outlets had accessed an email account said to have been used by the culprit several times.

16 **15th:** There was an incident in which Footprint Computer Solutions, the ccTLD registrar for Kenya's .ke domains, was accessed without authorization by an unknown party, leading to the hijacking of domains for several prominent sites such as Google and MSN.

17 **17th:** Oracle released a scheduled update for Java SE JDK and JRE, fixing 42 vulnerabilities including those that allowed execution of arbitrary code.
"Oracle Java SE Critical Patch Update Advisory - April 2013" (http://www.oracle.com/technetwork/topics/security/javacpuapr2013-1928497.html).

18 **17th:** Oracle released their quarterly scheduled update, which fixed a total of 86 vulnerabilities in multiple products such as Oracle and MySQL.
"Oracle Critical Patch Update Advisory - April 2013" (http://www.oracle.com/technetwork/topics/security/cpuapr2013-1899555.html).

19 **18th:** Microsoft announced they would provide two-step verification for Microsoft account, to improve the security features for dealing with unauthorized access.
The Official Microsoft Blog, "Microsoft Account Gets More Secure" (http://blogs.technet.com/b/microsoft_blog/archive/2013/04/17/microsoft-account-gets-more-secure.aspx).

20 **19th:** The NIC for Kyrgyzstan's .kg domains was accessed without authorization, and multiple domains including well-known examples such as Google and PayPal were hijacked.

21 **19th:** A revision to the Public Offices Election Law that allowed the Internet to be used for electioneering was passed by the Upper House.

22 **23rd:** The Japan Aerospace Exploration Agency (JAXA) announced that its servers had been accessed without authorization by an external source on April 17, and there was a possibility that information related to operation of the International Space Station had been leaked.
"Unauthorized Access of JAXA Server" (http://www.jaxa.jp/press/2013/04/20130423_security_e.html).

23 **23rd:** A number of websites were compromised at Oman Telecommunications Company, one of the ccTLD registrars for Oman's .om domains, and domains for a number of well-known sites such as Google were hijacked.
Oman National CERT, "Signs of a DNS Cache Poisoning Attack" (http://www.cert.gov.om/media_news_details.aspx?news=20#.UgoN5pJzPkd).

24 **24th:** The Twitter account for the Associated Press was accessed without authorization, and false information disseminated. The impact from this included a temporary slump in stock prices at the New York Stock Exchange.

25 **25th:** A 15-year-old youth was arrested on suspicion of violating the Unauthorized Computer Access Law. He is alleged to have accessed the IDs of other individuals without authorization using Tor, and changed passwords and email addresses without permission.

26 **28th:** It was reported that an external email service account used by a high-ranking Japanese government official for personal business was accessed without authorization, and emails with viruses attached were sent to related parties.

27

28

29

30

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

*Dates are in Japan Standard Time

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

During this survey period, there were a large number of attempts to obtain user IDs and passwords, as well as unauthorized login attempts through identity fraud, which was thought to involve the use of lists. From April there were many attempts to log in to SNS, e-commerce, or corporate member-oriented service sites without authorization, as well as related incidents, in which lists consisting of ID and password combinations are believed to have been used. In a number of cases this resulted in damages such as points being used without authorization, or passwords being changed.

Additionally, there were multiple incidents in which lists themselves are thought to have been targeted, with server compromises that exploited vulnerabilities leading to data being leaked from servers, and files containing user names and passwords being found. In one of the incidents in which information was leaked, user IDs and passwords as well as personal information had been saved with the security codes used for credit card authorization*14. Due to this improper management of data, significant impact was felt by credit card companies in addition to users.

Brute force attacks targeting IDs and passwords, as well as attacks using lists such as those in the incidents mentioned above, have been occurring frequently for some time. However, in most cases these attacks were aimed at individual sites, and there are few past examples of large-scale attacks on multiple sites in Japan such as those seen recently. There have also been incidents in which the intent of the perpetrator is not known, such as testing of only the login authentication.

For the recent incidents, attacks are believed to have been made using lists of IDs and passwords obtained from somewhere, targeting users who use the same ID and password combination at other sites*15.

The risk of using the same ID and password at multiple websites such as this has been pointed out in the past. For example, "Observation results regarding unauthorized login attacks using continuous automatic entry programs" published by the National Police Agency in 2012 confirmed that 6.7% of users had reused passwords*16. The danger of reusing IDs and passwords is frequently identified, but in light of the recent incidents, the Telecom Information Sharing and Analysis Center Japan issued another alert*17.

See "1.4.3 Recurring Incidents of Unauthorized Login" for more information about these incidents.

■ Attacks on TLD

Numerous attacks on domain registries including ccTLD continue to occur, along with associated domain hijackings and information leaks. In April, an incident occurred in which Footprint Computer Solutions, the ccTLD registrar for Kenya's .ke domains, was accessed without authorization by an unknown party, leading to the hijacking of domains for several prominent sites such as Google and MSN. There were also hijackings of a number of well-known sites, such as Google and PayPal, after the NIC for Kyrgyzstan's .kg domains was accessed without authorization. Unauthorized access also took place at Oman Telecommunications Company, one of the ccTLD registrars for Oman's .om domains, resulting in the domain hijackings of several big-name sites such as Google. In addition to these, domains including .ug for Uganda and .bi for Burundi were subject to domain hijackings. In each of these incidents, domain hijackings targeted domains for companies of world renown such as Google and PayPal.

*14 For example, the "'Information Security Guide' for Credit Card Member Stores (Guide to PCI DSS / ISMS Compliance)" (http://www.isms.jipdec.or.jp/doc/JIP-ISMS118-20.pdf) published by JIPDEC indicates that security codes are included in the sensitive authentication data covered by Requirement 3 of the PCI DSS, meaning that merchants are prohibited from storing them.

*15 One of the affected companies indicated in its final report that, due to the number of passwords attempts for each login ID, it believed IDs and passwords for other services had been obtained fraudulently and were being tested to see if they would work.

*16 National Police Agency, "Publication of the Status of Unauthorized Access Incidents in 2011" (http://www.npa.go.jp/cyber/statics/h23/pdf040.pdf) (in Japanese).

*17 Telecom Information Sharing and Analysis Center Japan, "[Alert] A spate of unauthorized use of user IDs / passwords, and recommended measures for users" (https://www.telecom-isac.jp/news/news20130412.html) (in Japanese).

May Incidents

S **1st:** The University of Toronto's Citizen Lab published its latest report on the FinSpy (FinFisher) commercial surveillance software, which the government agencies of various countries are thought to be using in their information-gathering activities.
See the following Citizen Lab report for more information. "For Their Eyes Only: The Commercialization of Digital Spying" (https://citizenlab.org/2013/04/for-their-eyes-only-2/).

V **4th:** Microsoft released a security advisory (2847140) regarding a vulnerability in IE8 for which no fix was available (CVE-2013-1347), which could allow remote code execution when a malicious website is viewed. This vulnerability was fixed in MS13-038 on May 15.
"Microsoft Security Advisory (2847140) Vulnerability in Internet Explorer Could Allow Remote Code Execution" (https://technet.microsoft.com/en-us/security/advisory/2847140).

S **8th:** Several hundred websites, including sites for U.S. government agencies and financial institutions, were affected by alterations, information leaks, and DDoS attacks coordinated by Anonymous (OpUSA).
Information on attack targets and details of the attacks can be confirmed in the following Pastebin statement. "#OpUSA target list" (http://pastebin.com/LXHKjsfg).

S **8th:** There were attempts to log in to an e-commerce site without authorization, with about 1,110,000 incidents of unauthorized access between May 4 and May 8. It was announced that login had been locked for approximately 15,000 user accounts for which unauthorized access had been confirmed. More information about these incidents was published on May 16, and a warning not to reuse passwords was issued after evidence pointed to the fact that lists of IDs and passwords obtained from other services were being used.

S **10th:** Eight members of a hacker group that compromised a credit card processing company in India, altered savings and withdrawal limit data, and stole 45 million dollars from ATMs around the world were indicted (Unlimited Operation).
See the following United States Attorney's Office for the Eastern District of New York statement for more information about this incident. "Eight Members Of New York Cell Of Cybercrime Organization Indicted In $45 Million Cybercrime Campaign" (http://www.justice.gov/usao/nye/pr/2013/2013may09.html).

O **11th:** Bloomberg L.P. admitted that Bloomberg News reporters had an inappropriate level of access to the data of customers using a financial information service provided by another one of its divisions, and announced they had undertaken corrective action.
See the following Bloomberg L.P. statement for more information. "Safeguarding Customer Data" (http://blog.bloomberg.com/2013-05-10/safeguarding-customer-data/).

V **15th:** Microsoft published their Security Bulletin Summary for May 2013, and released two critical updates, MS13-037 and MS13-038, as well as eight important ones including MS13-039.
"Microsoft Security Bulletin Summary for May 2013" (http://technet.microsoft.com/en-us/security/bulletin/ms13-May).

V **15th:** A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB13-14: Security updates available for Adobe Flash Player" (http://www.adobe.com/support/security/bulletins/apsb13-14.html).

V **15th:** A number of vulnerabilities in Adobe Reader and Acrobat that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB13-15 Security updates available for Adobe Reader and Acrobat" (http://www.adobe.com/support/security/bulletins/apsb13-15.html).

S **17th:** Yahoo! JAPAN announced that the servers managing Yahoo! JAPAN IDs had been accessed without authorization by an external source on May 16, and files containing only the extracted IDs of up to 22 million accounts may have been created and leaked. On May 23 it was also announced that some irreversibly encrypted passwords, as well as information required for resetting passwords when they are forgotten, may have been leaked for 1,480,000 accounts.
Yahoo! JAPAN, "Regarding Unauthorized Access to Our Servers" (http://pr.yahoo.co.jp/release/2013/0517a.html) (in Japanese). "Follow-up to 'Regarding Unauthorized Access to Our Servers' (published May 17)" (http://pr.yahoo.co.jp/release/2013/0523a.html) (in Japanese).

V **23rd:** A number of vulnerabilities in Apache Struts that could allow execution of arbitrary commands (CVE-2013-1965, CVE-2013-1966) were discovered and fixed.
The Apache Software Foundation, "S2-014 - A vulnerability introduced by forcing parameter inclusion in the URL and Anchor Tag allows remote command execution, session access and manipulation and XSS attacks" (http://struts.apache.org/release/2.3.x/docs/s2-014.html).

O **24th:** "The Bill on the Utilization of a Number to Identify Specific Individuals for Administrative Procedures (My Number Law)" was passed by the Upper House.
See the following Cabinet Secretariat site for more information. "The Social Security and Tax Number System" (http://www.cas.go.jp/jp/seisaku/bangoseido/english.html).

V **27th:** A number of vulnerabilities in Apache Struts that could allow execution of arbitrary commands (CVE-2013-1966, CVE-2013-2115) were discovered and fixed. Although CVE-2013-1966 had been fixed previously, it was fixed again due to the measures not being sufficient.

S **27th:** It was announced that the website for a company that rents mobile phones and mobile Wi-Fi routers to overseas travelers had been accessed without authorization on April 23, leading to the leak of up to 146,701 pieces of customer information, including credit card data such as security codes.

S **31st:** U.S. company Prolexic Technologies, which provides DDoS defense services, announced that it had prevented a 167 Gbps DDoS attack using DNS amplification against a financial exchange market system. 92% of the devices that participated in this attack were open resolvers.
"167 Gbps Attack Targeted Real-Time Financial Exchange Platform" (http://www.prolexic.com/news-events-pr-prolexic-stops-largest-ever-dns-reflection-ddos-attack-167-gbps.html).

S **31st:** The websites of the nic.mw and register.mw domain registries for Malawi were altered by an unknown party.

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

*Dates are in Japan Standard Time

After U.S. DNS registrar Moniker was accessed without authorization, they reset the passwords for all customer accounts due to the possibility that customer details including credit card information had been accessed. U.S. DNS hosting provider name.com also experienced unauthorized access, and responded to the possibility that customer information had been accessed by resetting all customer passwords*18. Incidents in which the websites for the nic.mw and register.mw domain registries that manage Malawi's .mw domains were altered by an unknown party have also occurred.

In June, DDoS attacks were carried out on authoritative DNS servers for a number of DNS hosting service providers, leading to service failures, etc. It is now known that these attacks were DDoS attacks made on other servers via DNS amplification using the authoritative DNS servers of these service providers*19. Another incident in June at U.S. firm Network Solutions resulted in approximately 5,000 domains appearing to have been hijacked due to an operation error during the response to a DDoS attack*20.

■ Attacks on Bitcoin

During the current survey period, there was a lot of discussion regarding a number of attacks made on the net-based Bitcoin virtual currency and its systems. The value of Bitcoin had been soaring in value, with the exchange rate against U.S. dollars reaching a high of $266 in April. As a result, there have been many incidents such as attacks and phishing attempts targeting Bitcoin. On April 3, the Mt.Gox Bitcoin exchange was the target of a DDoS attack, affecting service temporarily*21. Attacks that target Bitcoin indirectly are also on the rise, such as the discovery of malware that mines Bitcoin*22. Because the Bitcoin virtual currency can be exchanged anonymously, it can be used without disclosing your name, and it has been utilized for making donations to WikiLeaks, etc. On the other hand, issues have also been identified with its potential for use in crimes such as money laundering, so it must be used with care.

■ Government Agency Initiatives

Government agency initiatives included the Information Security Policy Council's conclusion of the "Cyber Security Strategy," which had been drawn up as a new basic strategy regarding information security to replace the "Information Security Strategy to Protect Citizens" established in 2010*23. To enhance systems for promotion, it was also decided that NISC (National Information Security Center) would become the "Cyber Security Center (provisional name)" by around FY2015, following implementation of the necessary functional improvements. "Cyber Security 2013" was also finalized based on this, summarizing specific initiatives to be implemented in FY2013 as an annual plan. These included improvements to the emergency response capability of government agencies, preparation of attack analysis capabilities, enhancements to functions for international collaboration, and improvements to human resource development and literacy levels*24.

Additionally, due to an increase in cyber attacks targeting government agencies and private-sector businesses, special units for investigating cyber attacks were established in 13 prefectures on April 1. In June it was also announced that a special cyber crime squad, consisting of investigators from the Cyber Crime Countermeasure Division of the Metropolitan Police Department's Community Safety Bureau and investigators dispatched from regional police, would be established in July to improve the efficiency of investigations. There were other moves to enhance systems for responding to cyber attacks, such as the Ministry of Defense announcing that it would establish a Cyberspace Defense Force (provisional name) in May, for improving the ability to implement comprehensive measures for countering cyber attacks on the systems and networks of the Ministry of Defense and the Self-Defense Forces. Furthermore, regarding the establishment of a National Security Council for planning foreign and security policy (in other words, a Japanese version of the NSC), the Act Regarding Establishment

*18 Name.com Blog, "We got hacked" (http://www.name.com/blog/general/2013/05/we-got-hacked/).

*19 See the following blog post from DNSimple, one of the companies affected, for more information about the attacks. "Incident Report: DNS Outage due to DDoS Attack" (http://blog.dnsimple.com/incident-report-dns-outage-due-to-ddos-attack/).

*20 See the following Cisco Blog for more information. "'Hijacking' of DNS Records from Network Solutions" (http://blogs.cisco.com/security/hijacking-of-dns-records-from-network-solutions/).

*21 See the following Mt.Gox statement for more information about this incident. "It's been an epic few days: What happened?" (https://www.mtgox.com/press_release_20130404.html).

*22 See the following Kaspersky Lab SECURELIST Blog post for more information about this malware. "Skypemageddon by bitcoining" (http://www.securelist.com/en/blog/208194210/Skypemageddon_by_bitcoining).

*23 National Information Security Center, "Information Security Policy Council - 32nd Assembly" (June 10, 2013) (http://www.nisc.go.jp/conference/seisaku/index.html#seisaku35) (in Japanese).

*24 National Information Security Center, "Information Security Policy Council - 32nd Assembly" (June 27, 2013) (http://www.nisc.go.jp/conference/seisaku/index.html#seisaku36) (in Japanese).

June 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

S **4th:** DDoS attacks were made on authoritative DNS servers for a number of DNS hosting services, such as DNSimple and easyDNS, causing service failures, etc.
For more information, see the following announcements from TPP Wholesale Pty Ltd, which was one of those targeted. "Unscheduled Service Interruption - TPP Wholesale DNS - 3rd June 2013" (http://www.tppwholesale.com.au/support/service-alerts/unscheduled-service-interruption-tpp-wholesale-dns-3rd-june-2013). "More information on recent DDoS attacks - June 2013" (http://www.tppwholesale.com.au/support/service-alerts/more-information-recent-ddos-attacks).

V **5th:** A vulnerability (CVE-2013-3919) in BIND 9.x that could allow external parties to cause a crash using specially crafted data was discovered and fixed.
Internet Systems Consortium, "CVE-2013-3919: A recursive resolver can be crashed by a query for a malformed zone" (https://kb.isc.org/article/AA-00967/).

V **5th:** A number of vulnerabilities in Apache Struts that could allow execution of arbitrary commands (CVE-2013-2134, CVE-2013-2135) were discovered and fixed.
The Apache Software Foundation, "S2-015 - A vulnerability introduced by wildcard matching mechanism or double evaluation of OGNL Expression allows remote command execution." (http://struts.apache.org/release/2.3.x/docs/s2-015.html).

V **6th:** A vulnerability in Parallels Plesk Panel versions 9.0 - 9.2.3 that could allow remote arbitrary code execution was disclosed on a security-related mailing list. Because this vulnerability only affects old versions for which support has already ended, users have been urged to upgrade to a newer version.
Parallels, "Parallels Plesk Panel: phppath/PHP vulnerability" (http://kb.parallels.com/116241).

S **6th:** Microsoft announced it had uncovered the Citadel botnet together with a number of partners such as the FBI and FS-ISAC.
"Microsoft, financial services and others join forces to combat massive cybercrime ring" (http://www.microsoft.com/en-us/news/Press/2013/Jun13/06-05DCUPR.aspx).

O **7th:** JPCERT/CC issued an alert regarding a spate of website alteration incidents in Japan. About 1,000 incidents have been reported since April 2013, with most altered websites used to redirect users to attack sites.
"JPCERT/CC Alert 2013-06-07 Alert regarding compromised websites" (http://www.jpcert.or.jp/english/at/2013/at130027.html).

V **12th:** Microsoft published their Security Bulletin Summary for June 2013, and released the MS13-047 critical update as well as four important ones including MS13-051.
"Microsoft Security Bulletin Summary for June 2013" (http://technet.microsoft.com/en-us/security/bulletin/ms13-Jun).

O **12th:** The Ministry of Internal Affairs' Research Society for Use and Circulation of Personal Data published a report summarizing the results of their evaluation of the proper use of big data that includes personal data, and the circulation of information required for providing highly-convenient services taking privacy into consideration.
"Official Announcement of Report from Research Society for Use and Circulation of Personal Data" (http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/130612_06.html).

V **13th:** A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB13-16: Security updates available for Adobe Flash Player" (http://www.adobe.com/support/security/bulletins/apsb13-16.html).

O **14th:** U.S. ICS-CERT issued an alert encouraging proper management and access restrictions for approximately 300 medical devices from 40 vendors, due to hard-coded passwords being used.
"Alert (ICS-ALERT-13-164-01) Medical Devices Hard-Coded Passwords" (http://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01).

V **18th:** A vulnerability in Ichitaro that allowed arbitrary code execution was discovered and fixed.
*JustSystems Corporation, "[JS13002] Regarding the Risk of Malicious Program Execution Exploiting a Vulnerability in Ichitaro" (http://www.justsystems.com/jp/info/js13002.html) (in Japanese).

S **18th:** It was announced that a group that had compromised a port system in Antwerp and smuggled weapons and drugs had been apprehended through a joint investigation conducted by multiple agencies in the Netherlands and Belgium.
See the following statement from Dutch prosecutors for more information about this incident. "Drugshandelaren hacken rederijen en ontvreemden containers met cocaïne" (http://www.om.nl/actueel/nieuws-persberichten/@161061/drugshandelaren/) (in Dutch).

V **19th:** Oracle released their quarterly scheduled update for Java SE JDK and JRE, fixing 40 vulnerabilities including those that allowed execution of arbitrary code.
"Oracle Java SE Critical Patch Update Advisory - June 2013" (http://www.oracle.com/technetwork/topics/security/javacpujun2013-1899847.html).

V **19th:** A vulnerability in the Flash plug-in for Google Chrome that could allow a third party to obtain important information from the physical environment of a machine via methods such as clickjacking attacks was discovered and fixed. This was caused by proper authority management not being carried out in Flash applications.
"Stable Channel Update" (http://googlechromereleases.blogspot.jp/2013/06/stable-channel-update_18.html).

S **19th:** On June 26, Opera stated it had been compromised in a targeted attack, resulting in the theft of code signing certificates. They also announced that between 10:00 and 10:36 AM Japan time, several thousand Windows users may have been affected when an update file using fraudulent certificates was distributed using the automatic update system.
The Opera Security group, "Security breach stopped" (http://my.opera.com/securitygroup/blog/2013/06/26/opera-infrastructure-attack).

S **21st:** An accident occurred at U.S. company Network Solutions, causing about 5,000 domains to appear as if they had been hijacked due to operation error when responding to a DDoS attack. See the following Cisco Blog for more information about this incident.
"'Hijacking' of DNS Records from Network Solutions" (http://blogs.cisco.com/security/hijacking-of-dns-records-from-network-solutions/).

V **22nd:** A vulnerability in Facebook's Download Your Information tool that unintentionally exposed the contact details for some users was fixed.
"Important Message from Facebook's White Hat Program" (https://www.facebook.com/notes/facebook-security/important-message-from-facebooks-white-hat-program/10151437074840766).

V **22nd:** 12 vulnerabilities in WordPress were fixed, including a fix for server-side request forgeries that could allow attackers to gain access to a site.
WordPress.com Blog, "WordPress 3.5.2 Maintenance and Security Release" (http://wordpress.org/news/2013/06/wordpress-3-5-2/).

S **25th:** Charges were filed against a number of journalists suspected of accessing an email account thought to have been used by the culprit in relation to the Remote Control Virus incident.

S **25th:** In South Korea, website alterations and DDoS attacks were made on a number of government-related websites and corporate websites. There were also multiple system failures thought to be caused by malware.
See the following Trend Micro SECURITY BLOG post for more information. "More large-scale cyber attacks on South Korea: What happened? What lessons should we take from this?" (http://blog.trendmicro.co.jp/archives/7462) (in Japanese).

O **28th:** Adobe announced it had prepared a system that allows easy verification of Local Government Public Key Infrastructure (LGPKI) digital signatures in Adobe Reader and Acrobat as part of its cyber attack countermeasures, in response to LGPKI initiatives for the digital signing of PDF files.
"Adobe Systems Cooperates in Local Authorities Systems Development Center's Cyber Attack Countermeasures" (http://www.adobe.com/jp/aboutadobe/pressroom/pressreleases/20130628_LGPKI.html) (in Japanese).

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

*Dates are in Japan Standard Time

of a National Security Council was approved by the Cabinet following a Meeting of Key Figures Regarding Establishment of a National Security Council*25.

Other

In April, a revision to the Public Offices Election Law making it possible to use the Internet for electioneering was passed. This allowed candidates and political parties to conduct electioneering over the Internet using services such as Facebook and Twitter. On the other hand, it must be noted that there are also certain restrictions on the Internet activities of eligible voters, such as electioneering via email being prohibited*26.

Regarding the series of incidents concerning the Remote Control Virus that made headlines from October of last year, the investigation into the suspect arrested in February eventually resulted in him being charged with crimes such as fraudulent obstruction of business in relation to seven incidents. In connection to this, criminal papers were filed with prosecutors against a number of journalists on suspicion of accessing an email account thought to have been used by the culprit behind the Remote Control Virus incident last October.

In June, an article regarding the activities of the U.S. National Security Agency (NSA) released by a U.K. newspaper publisher stirred up a lot of buzz. The NSA has been gathering information related to terrorism for some time, but it was reported that U.S. citizens were also being targeted in surveillance, and in addition to collecting phone records, a program called PRISM that monitors data such as Internet-based videos, photos, and emails was being run with the cooperation of major U.S. companies associated with the Internet. For this reason, a number of companies whose involvement was indicated explained that they were legally compelled to provide the data, and published details of the number of requests for data disclosure received from government agencies. There were also reports that the NSA may be eavesdropping on the fiber optic cable networks used to convey Internet traffic, and gathering information at locations such as international conferences. These activities were criticized both in the U.S. and other countries around the world, including the EU, and there are concerns they could affect foreign diplomacy.

On June 25, an incident occurred in which multiple government-related websites and corporate websites in South Korea were altered, and DDoS attacks made on DNS servers. It appears that attacks were carried out simultaneously by a number of attackers, and there were several Web alterations thought to have been instigated by Anonymous and system failures believed to be caused by malware. These attacks are suspected to be related to the 3.20 Cyber Attack that took place in March due to similarities between the attacks*27.

*25 Office of the Prime Minister, "Meeting of Key Figures Regarding Establishment of a National Security Council" (http://www.kantei.go.jp/jp/singi/ka_yusiki/) (in Japanese).

*26 See the following Ministry of Internal Affairs and Communications site for more information about electioneering activities associated with revisions to the law "Information regarding Removal of the Ban on Internet Electioneering" (http://www.soumu.go.jp/senkyo/senkyo_s/naruhodo/naruhodo10.html) (in Japanese).

*27 The malware used in the latest incidents had several similar features, such as initiating attacks at a predetermined time. See the following Symantec Security Response blog for more information on the behavior of the malware. "Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War" (http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war).

1.3 Incident Survey

1.3.1 DDoS Attacks

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

■ Direct Observations

Figure 2 shows the circumstances of DDoS attacks handled by the IIJ DDoS Defense Service between April 1 and June 30, 2013.

This information shows traffic anomalies judged to be attacks based on IIJ DDoS Defense Service standards. IIJ also responds to other DDoS attacks, but these incidents are excluded from the figure due to the difficulty in accurately ascertaining the facts of each situation.

There are many methods that can be used to carry out a DDoS attack, and the capacity of the environment attacked (bandwidth and server performance) will largely determine the degree of impact. Figure 2 categorizes DDoS attacks into three types: attacks on bandwidth capacity*28, attacks on servers*29, 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 514 DDoS attacks. This averages to 5.65 attacks per day, indicating a decrease in the average daily number of attacks compared to our prior report. Server attacks accounted for 98.1% of all incidents, and compound attacks accounted for the remaining 1.9%. There were no bandwidth capacity attacks.

The largest attack observed during the period under study was classified as a server attack, and resulted in 295 Mbps of bandwidth using up to 55,000 pps packets.

Of all attacks, 78.8% ended within 30 minutes of commencement, 21% lasted between 30 minutes and 24 hours, and 0.2% lasted over 24 hours. The longest sustained attack was a server attack that lasted for two days, six hours, and 37 minutes (54 hours and 37 minutes).

In most cases, we observed an extremely large number of IP addresses, whether domestic or foreign. We believe this is accounted for by the use of IP spoofing*30 and botnet*31 usage as the method for conducting DDoS attacks.

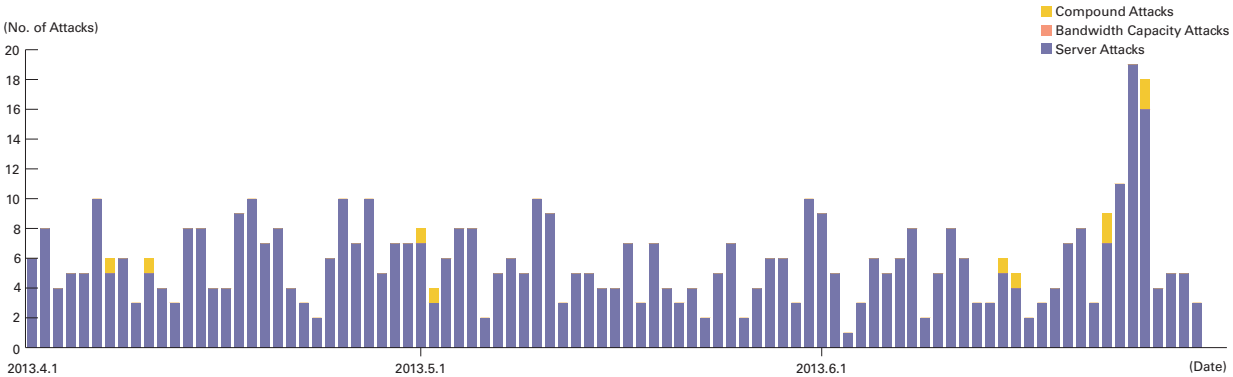


Figure 2: Trends in DDoS Attacks

*28 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.

*29 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.

*30 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.

*31 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*32 set up by the MITF, a malware activity observation project operated by IIJ*33. 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 April 1 and June 30, 2013, Figure 3 shows the sender's IP addresses classified by country, and Figure 4 shows trends in packet numbers by port.

The port most commonly targeted by the DDoS attacks observed was the 80/TCP port used for Web services, accounting for 51.8% of the total during the target period. Attacks were also observed on ports such as 53/TCP used for DNS and 22/TCP for SSH, as well as the game-related 25565/TCP, and the typically unused 6010/TCP and 6005/TCP.

Particularly large numbers of backscatter packets observed included those from a number of Web servers (80/TCP) on April 2, when attacks on the Web servers of a science-related site in Canada and U.S. hosting providers were observed. On May 17, attacks on the Web servers of another U.S. hosting provider were also detected. Attacks on Web servers for a security provider in Germany were observed on June 3. On June 5, attacks were observed targeting the Web servers of a U.S. hosting provider and a Chinese e-commerce vendor.

Many attacks targeting SSH (22/TCP) were also observed, including those on the servers for Swiss, U.S., and Dutch hosting providers. Attacks on 25565/TCP, thought to be related to games, were observed targeting a number of hosting providers in the United States.

Between April 30 and May 1, a large number of attacks on 2106/TCP against a U.S. hosting provider were observed. Attacks on 6010/TCP targeting servers for a Dutch hosting provider were observed between May 21 and May 30. These attacks were not concentrated on a particular day, and continued for some time, with a total of over 10,000 observed within this period. These ports are not normally used by standard applications, so the purpose of the attacks is not known. Notable DDoS attacks during the current survey period that were detected via IIJ's observations of backscatter included attacks on sites related to North Korea in April thought to have been made by Anonymous. In May, there were attacks on U.S. government agencies and financial institutions, and in June a number of attacks

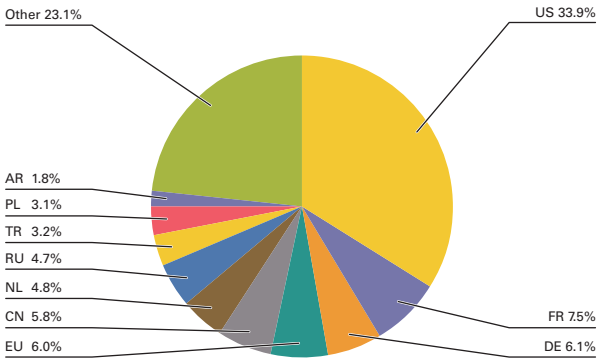


Figure 3: Distribution of DDoS Attack Targets According to Backscatter Observations (by Country, Entire Period under Study)

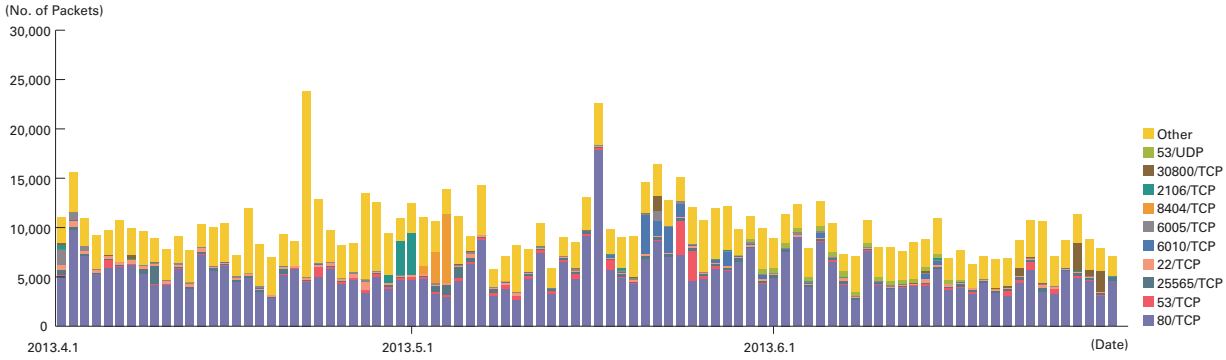


Figure 4: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)

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

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

on Swedish government agencies were observed. Backscatter thought to be from attacks on Israeli intelligence agencies, attacks on the websites of well-known U.S. security specialists between May and June, attacks on a religious group in the U.S. that exhibits radical behavior, and attacks on MIT were detected.

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the MITF*34, a malware activity observation project operated by IIJ. The MITF uses honeypots*35 connected to the Internet in a manner similar to general users in order to observe communications arriving over the Internet. Most appear to be communications by malware selecting a target at random, or scans attempting to locate a target for attack.

■ Status of Random Communications

Figure 5 shows the distribution of sender's IP addresses by country for communications coming into the honeypots between April 1 and June 30, 2013. Figure 6 shows trends in the total volumes (incoming packets). The MITF has set up numerous honeypots for the purpose of observation. We have taken the average per honeypot, showing the trends for incoming packet types (top ten) over the entire period subject to study. Additionally, in these observations we corrected data to count multiple TCP connections as a single attack when the attack involved multiple connections to a specific port, such as attacks on MSRPC.

Much of the communications arriving at the honeypots demonstrated scanning behavior targeting TCP ports utilized by Microsoft operating systems. We also observed scanning behavior targeting 1433/TCP used by Microsoft's SQL Server, 3389/TCP used by the RDP remote login function for Windows, 22/TCP used for SSH, 3306/TCP used for MySQL, and ICMP echo requests. Additionally, communications of an unknown purpose were observed on ports not used by common applications, such as 6666/TCP and 56994/UDP.

Communications thought to be SSH dictionary attacks also occurred during the current survey period. For example, concentrated communications were observed coming from IP addresses allocated to India, China, and South Korea on April 12, and from IP addresses allocated to South Korea on April 15. 56994/UDP communications targeting a specific honeypot IP address from an IP address allocated to Iran also took place on April 6. Because both the data lengths and the data itself were random, the purpose of this is not known. Between late April and mid-May, there was an increase in communications targeting 6666/TCP to 6675/TCP on a wide range of honeypot IP addresses. This

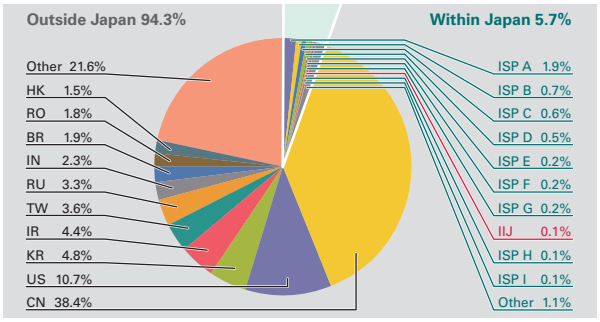


Figure 5: Sender Distribution (by Country, Entire Period under Study)

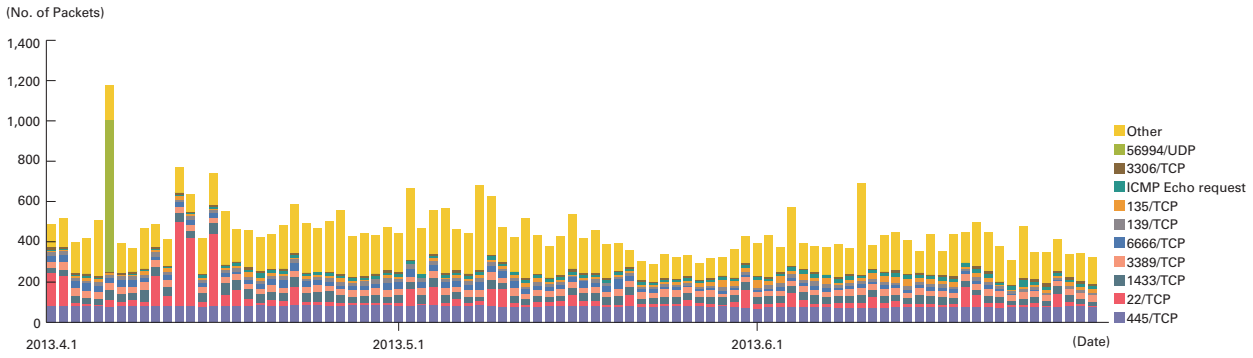


Figure 6: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

*34 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.

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

was mainly from China and the United States. 6667/TCP is a port used for IRC, and because some IRC clients use ports in this range, we believe this to be related scanning behavior.

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.

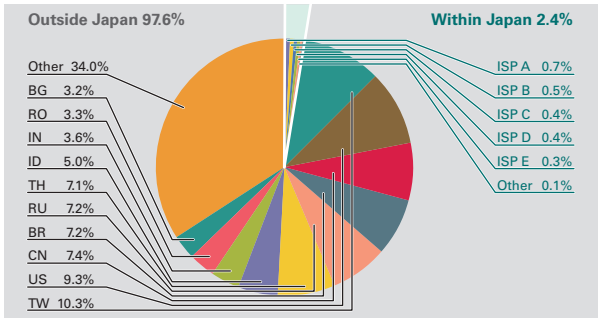


Figure 7: Distribution of Acquired Specimens by Source (by Country, Entire Period under Study, Excluding Conficker)

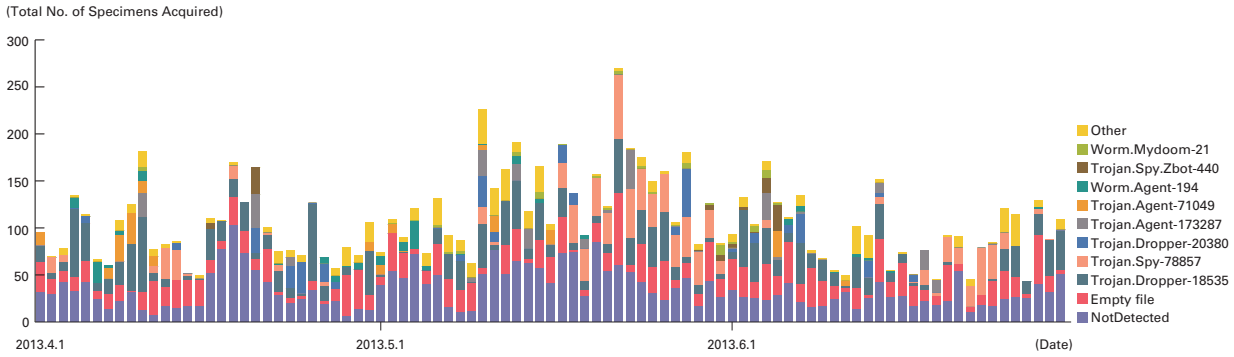


Figure 8: Trends in the Total Number of Malware Specimens Acquired (Excluding Conficker)

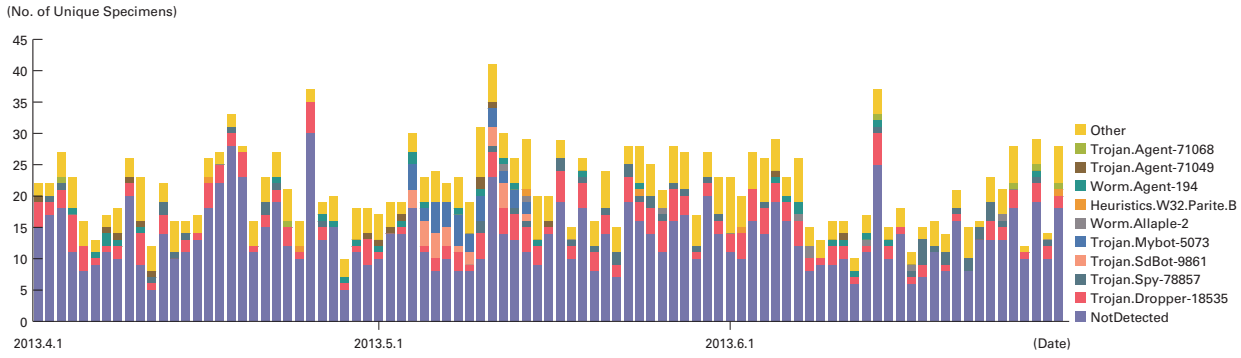


Figure 9: Trends in the Number of Unique Specimens (Excluding Conficker)

*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.

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

On average, 109 specimens were acquired per day during the period under study, representing 22 different malware. After investigating these undetected specimens more closely, we learned malware*38 that steals accounts had been observed on an ongoing basis in Indonesia and the Philippines in April. Two bot variants*39*40 controlled by IRC servers were also observed intermittently in the same regions in May and June, and a worm*41 sourced to IP addresses allocated to the U.S. and Hong Kong was observed in the U.S. and France in early April and late June.

Under the MITF's independent analysis, during the current period under observation 40.4% of malware specimens acquired were worms, 53.2% were bots, and 6.4% were downloaders. In addition, the MITF confirmed the presence of 120 botnet C&C servers*42 and 15 malware distribution sites. The number of C&C servers has risen dramatically since the last report, but this is due to the presence of a single type of malware with a DGA (Domain Generation Algorithm)*43 function. IIJ analysis indicates that the domains this malware generates use a "www.(6 random letters).com" format.

■ Conficker Activity

Including Conficker, an average of 33,250 specimens were acquired per day during the period covered by this report, representing 791 different malware. While figures rise and fall over short periods, Conficker accounts for 99.7% of the total number of specimens acquired, and 97.3% of unique specimens. This demonstrates that Conficker remains the most prevalent malware by far, so we have omitted it from figures in this report.

The total number of specimens acquired during the period covered by this report increased by approximately 13% compared to the previous survey period. Unique specimens were also down by about 2%. According to the observations of the Conficker Working Group*44, as of June 30, 2013, a total of 1,312,964 unique IP addresses are infected. This is a drop of approximately 41% compared to the 3.2 million PCs observed in November 2011, but it demonstrates that infections are still widespread.

*38 Trojan:Win32/Neurevt.A (http://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Trojan%3AWin32%2FNeurevt.A).
*39 Trojan:Win32/Ircbrute (http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?name=Trojan%3AWin32%2FIrcbrute).
*40 Win32/Hamweq (http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fHamweq).
*41 WORM_DEBORM. AP (http://about-threats.trendmicro.com/Malware.aspx?id=36201&name=WORM_DEBORM.AP&language=au).
*42 An abbreviation of Command & Control Server. A server that provides commands to a botnet consisting of a large number of bots.
*43 DGA (Domain Generation Algorithm) refers to systems in which malware automatically generates a domain name for the C&C server to connect to based on a fixed rule, such as the time. This is used to avoid URL filtering devices, and to recover and resume activity after the connected C&C server is shut down by generating a new domain name and reconnecting.
*44 Conficker Working Group Observations (http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking).

1.3.3 SQL Injection Attacks

Of the types of different Web server attacks, IIJ conducts ongoing surveys related to SQL injection attacks*45. SQL injection attacks have flared up in frequency numerous times in the past, remaining one of the major topics in the Internet security. SQL injections are known to occur in one of three attack patterns: those that attempt to steal data, those that attempt to overload database servers, and those that attempt to rewrite Web content.

Figure 10 shows the distribution of SQL injection attacks against Web servers detected between April 1 and June 30, 2013. Figure 11 shows trends in the numbers of attacks. These are a summary of attacks detected by signatures on the IIJ Managed IPS Service.

Japan was the source for 31.1% of attacks observed, while the United States and China accounted for 21.8% and 19.1%, respectively, with other countries following in order. Fewer SQL injection attacks were made against Web servers compared to the previous report. Attacks from China rose to 3rd place, due to large-scale attacks on specific targets that occurred on some days.

During this period, there were large-scale attacks from a number of attack sources including the U.S. and the Netherlands directed at specific targets between May 1 and May 2. On May 2, attacks from specific attack sources in the United States directed at a specific target also took place. There were also attacks from specific attack sources in China directed at specific targets on April 19, attacks on the same specific targets from a number of attack sources in China on June 3, and attacks on specific attack targets from a number of attack sources thought to be from Tor on June 9. Additionally, there were attacks from specific attack sources in China directed at a number of targets on June 27. These attacks are thought to have been attempts to find vulnerabilities on a Web server.

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

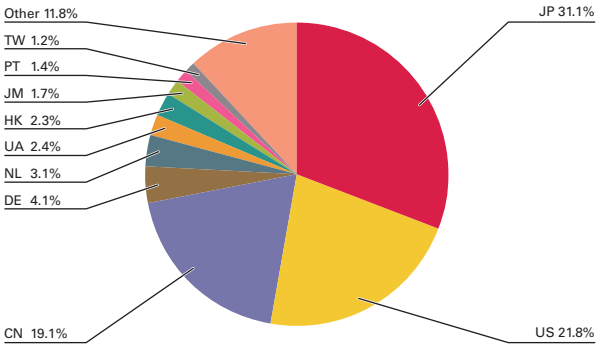


Figure 10: Distribution of SQL Injection Attacks by Source

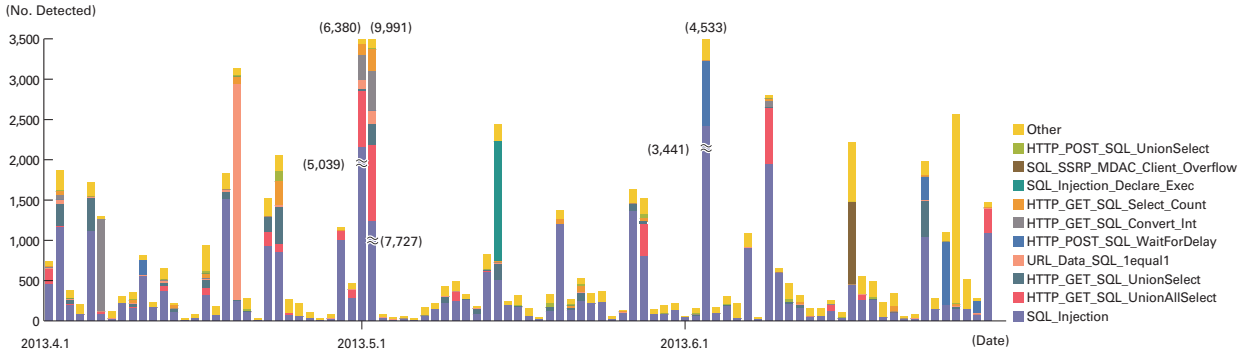


Figure 11: Trends in SQL Injection Attacks (by Day, by Attack Type)

*45 Attacks accessing a Web server to send SQL commands, thereby manipulating an underlying database. Attackers access or alter the database content without proper authorization, and steal sensitive information or rewrite Web content.

1.4 Focused Research

Incidents occurring over the Internet change in type and scope from one minute to the next. Accordingly, IIJ works toward implementing countermeasures by continuing to perform independent surveys and analyses of prevalent incidents. Here, we present information from the surveys we have undertaken during this period covering three themes. First, we take a look at techniques for detecting the ZeroAccess malware. Next, we examine the potential risks of home routers being exploited. Finally, we discuss the recent spate of unauthorized login incidents.

1.4.1 An Examination of ZeroAccess and its IOC

ZeroAccess is a bot-type malware that began to emerge from around 2009. In September of last year, Sophos published an analysis report regarding ZeroAccess*46. The report stated that 9 million computers worldwide had been infected with ZeroAccess up to that point, and provided infected node ratios for each country. It indicated that a large number of computers in Japan were also affected at the time. The main purpose of the malware was monetary exploitation through click fraud and Bitcoin mining on infected computers. However, ZeroAccess is equipped with a function for executing DLL plug-ins just like SpyEye and ZeuS variants*47, so new features may be incorporated in the future.

In this section, we explain the behavior of recent ZeroAccess variants analyzed by IIJ, and share our findings regarding the IOC (Indicators of Compromise)*48 for detecting them on infected computers.

■ Behavior of ZeroAccess User Mode Variants

In many cases, ZeroAccess is installed via drive-by downloads*49 using exploit kits*50 such as Blackhole, or using social engineering techniques by distributing it as fake cracked software. In recent years, implementations of ZeroAccess variants have begun to differ dramatically from those first seen, with some forming botnets via P2P, and others only operating in user

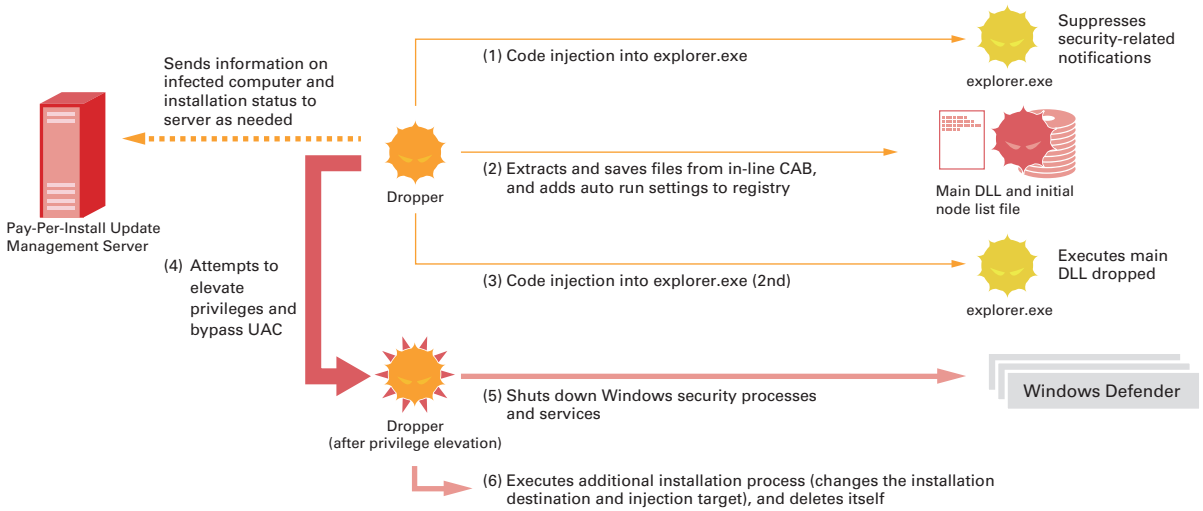


Figure 12: Behavior of ZeroAccess User Mode Variants (Dropper)

*46 In its report, Sophos noted that Japan had the 3rd highest ratio for infection of super nodes (nodes with global IP addresses directly accessible from other infected nodes), and the 10th highest ratio for infection of non-super nodes. "The ZeroAccess Botnet: Mining and Fraud for Massive Financial Gain" (http://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/Sophos_ZeroAccess_Botnet.pdf).

*47 See IIR Vol.13 under "1.4.2 SpyEye" (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol13_EN.pdf) for more information about SpyEye. Additionally, see IIR Vol.16 under "1.4.3 ZeuS and its Variants" (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol16_EN.pdf) or IIR Vol.18 under "1.4.2 The Citadel Variant of ZeuS" (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol18_EN.pdf) for an explanation of ZeuS behavior and its variants.

*48 An IOC (Indicator of Compromise) is technical information indicating the existence of known threats.
For malware, IOCs are defined based on the characteristics of the communications carried out, as well as the changes that they make to OS artifacts. Once an IOC related to malware is defined, subsequent incidents of infection with the same malware can be dealt with swiftly. IOC standards include OpenIOC, CybOX, and IODEF. The following presentation made by Chris Harrington at RSA Conference 2013 compares the good and bad points of each standard. "Sharing Indicators of Compromise: An Overview of Standards and Formats" (http://www.rsaconference.com/writable/presentations/file_upload/dsp-w25a.pdf).

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

*50 Exploit kits were explained during IIJ Technical Week 2010. "IIJ Technical WEEK 2010 Security Trends for 2010 (1) Web Infection Malware Trends" (http://www.iij.ad.jp/company/development/tech/techweek/pdf/techweek_1119_1-3_hiroshi-suzuki.pdf) (in Japanese).

mode. User mode variants of ZeroAccess consist of a dropper, and a DLL installed by the dropper. Figure 12 and Figure 13 give an outline of ZeroAccess user mode variant behavior*51.

The dropper executes code that disables some Windows security functions in many places, allowing installation to proceed smoothly. For example, it shuts down processes related to Windows security such as MSASCui.exe and wscntfy.exe, injects code into explorer.exe, and hooks the entries for wscntfy.dll and actioncenter.dll in the IAT to suppress security-related notifications. After bypassing UAC by exploiting the DLL load order*52, it shuts down a large number of processes and services related to security. The dropper also communicates with external sources frequently during the installation process, sending information on infected computers and the installation status. This is thought to be for collecting the information necessary for pay-per-install services*53.

Subsequently, the installed DLL connects to the ZeroAccess P2P network based on the initial node list file. It then sends and receives bot commands via UDP, and downloads and uploads plug-in files over TCP. The click fraud and Bitcoin mining functions mentioned above are executed using plug-ins, so the installed DLL itself mainly carries out communications with other peers. ZeroAccess verifies plug-in files by extracting metadata such as size and time stamp as well as signature from the Extended Attribute (EA) included in the entry information of the NTFS file system. It also extracts and verifies the signature relating to data from the resource section of a file. This makes it difficult for third parties other than the creator of ZeroAccess to upload an arbitrary executable file, and make other peers download and execute it.

■ IOC-related Observations

Here we will take a brief look at the IOC for detecting ZeroAccess variants on infected computers, based on its behavior detailed above. The most commonly used elements for IOC definitions are file names, file hash values, registry keys, and URLs. However, personally I do not recommend that this information be defined. This is because they are merely superficial pieces of data that are not directly related to the behavior of malware. The DLL installation path for ZeroAccess user mode variants actually differs depending on the variant.

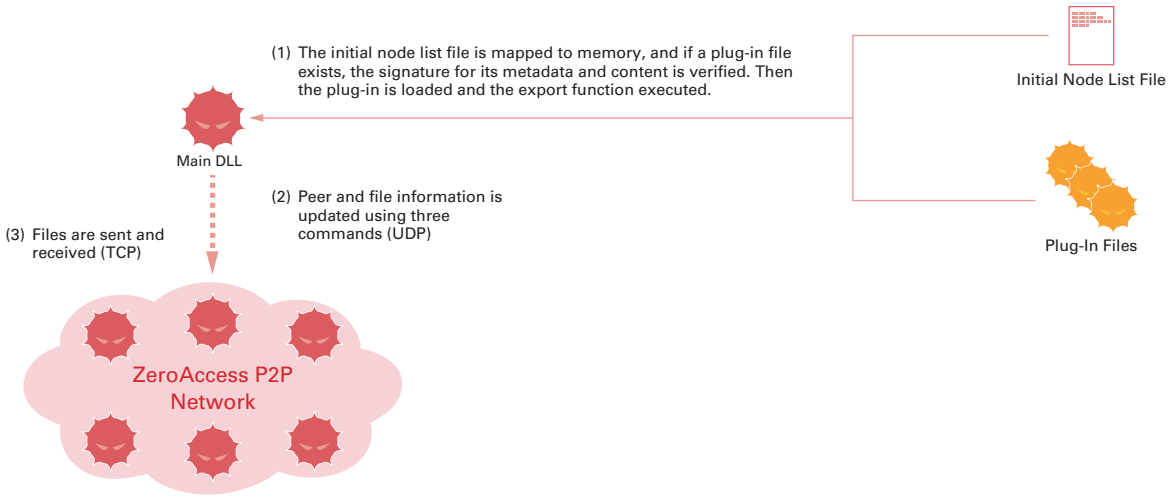


Figure 13: Behavior of ZeroAccess User Mode Variants (Installed DLL)

*51 In addition to the variants explained here, IIJ has also confirmed another variant that applies a patch to services.exe, but we have found that the basic behavior is the same.

*52 In recent variants, an Adobe Flash installer is stored in a CAB in the data area of the dropper. The dropper first extracts this to a temporary folder, then saves itself under the file name, "msimg32.dll" (the same file name used for a DLL in the Adobe Flash installer). Next, a UAC prompt is displayed upon execution of the installer, and if the user selects "Yes" the dropper is executed again with elevated privileges.

*53 Pay-per-install is a system in which money is paid based on the number of computers malware is installed on. The amount paid differs depending on a variety of information on the infected computer, such as the GeoIP, the OS version, and the type of privileges gained. The Sophos report mentioned above indicates that this pay-per-install service system is one of the factors increasing the number of computers infected with ZeroAccess. See the following presentation by Juan Caballero at USENIC Security '11 for market research and observations on pay-per-install services. "Measuring Pay-per-Install: The Commoditization of Malware Distribution" (http://usenix.org/events/sec11/tech/full_papers/Caballero.pdf).

By defining information that relates to malware behavior, the IOC is more generic, and can be used to detect a greater number of variants. For example, the installed DLL sends and receives bot commands over UDP, and these command names are defined using a 4-byte string*54. These are fixed unless a completely different P2P protocol is used. Furthermore, when commands are sent and received, XOR encryption based on a 4-byte key is used on the payload. The same key must be used by both parties communicating, so this is another value that is unlikely to change. The API*55 that ZeroAccess imports can also be defined as a characteristic. A generic IOC can be generated by combining information such as this.

Compression known as generic packing is used for the malware on the file system, so when applying IOC based on the information mentioned above, the target must be a binary image of the volatile memory data. For ZeroAccess, one thing that should be noted here is that the dropper and the installed DLL are completely different executable files. The dropper deletes itself once the DLL is installed, so even if the characteristics of the dropper are defined, it is not realistically possible to detect it in the memory image. The dropper contains a lot of distinctive code, such as API function calls or data acquisition via the call/jmp commands used in the PIC (Position-Independent Code)*56, code for extending the stack area dynamically, and code for tricky deletion processing*57. However, these cannot be used as IOC.

Here we have taken a look at the behavior of ZeroAccess user mode variants, and discussed its IOC. However, it is also possible to generate generic IOC for the kernel mode ZeroAccess that appeared earlier, using elements such as the API imported by its driver.

■ Summary

In this section, we explained the behavior of ZeroAccess, and took a quick look at generic IOC for detecting it on infected computers. The main infection vectors for ZeroAccess are drive-by downloads using exploit kits, and the execution of fake programs distributed over the Internet. This means that points we have emphasized in this IIR to date are crucial for preventing infection. Namely, it is necessary to keep software up to date, including that from third parties, and stay vigilant by not executing programs that cannot be trusted without thorough consideration.

Additionally, as demonstrated by the behavior of ZeroAccess, the malware of late disables Windows security functions and anti-virus software. Consequently, once you are infected, it will take a long time to detect this in many cases. This applies all the more when a large number of computers must be checked. In cases like this, being able to detect threats quickly using IOC can lead to the swift resolution of an incident. IOCs also use a fixed format, so they can be shared easily. This means that those without specialist knowledge of malware can also take part in investigations. The approach of using defined IOC when responding to an incident is not taken often in Japan at the moment, but as shown here there are many advantages to it, so I would recommend everyone give it a try.

*54 Command types include Lteg (initiates communication: then receives responses, updates peer info, and downloads files), Lter (response to Lteg: includes some peer and file information), and Lwen (broadcasts new peers to botnet).

*55 For example, ZeroAccess uses comparatively low-layer APIs such as ZwQueryInformationThread and ZwQueueApcThread when injecting code, and ZwDeleteValueKey and ZwCreateFile for registry and file operations.

*56 Code designed to be able to carry out the intended operation regardless of the current execution status, like shell code.

*57 It obtains the shell path (normally cmd.exe) by searching for environment variables, launches the shell in a suspended state, and then changes the execution context and stack of the shell process to delete the dropper being executed.

1.4.2 Home Router Security

A DDoS attack on a European anti-spam organization in March 2013 was of a previously unheard of scale, peaking at 300 Gbps*58. This used DNS amplification attack (details below) techniques, and is said to have reached this scale by using DNS servers and home routers*59 with configuration issues as stepping stones*60.

Here we summarize the current state of home routers generally used in households, discuss the cause of this situation, and consider measures for resolving it.

■ Home Router-Related Incidents

First, we will look at attacks targeting home routers that have occurred over the past few years, as well as incidents related to home routers.

■ Changes to DNS Settings by Exploiting Vulnerabilities

In 2011, it came to light that a vulnerability affecting a number of home routers (ADSL modems) had been exploited to change their settings to reference malicious DNS servers that had been prepared by an unknown party*61. It is said that up to 4.5 million units around the world had been compromised fraudulently using this technique. The malicious DNS servers returned fraudulent responses during the name resolution of sites for institutions such as banks, redirecting users to fake servers. This led to damages such as the theft of IDs and passwords for online banking, and the installation of malicious software.

■ Unauthorized Access to Management Interfaces

Some home routers do not implement any access restrictions under their default settings. This leads to the issue of it being possible to log in from anywhere on the Internet with administrator privileges when the default administrator ID and password are used*62. In most cases routers were equipped with access control functions, and the manual contained instructions that encourage users to configure them. However, because users had not changed the settings or password since the time of installation, it was possible to access the router with administrator privileges.

It is also known that some devices save authentication information (for example, the ID and password for connecting to an ISP) to the router in plain text. Consequently, there have been incidents in which an external party has accessed a device with administrator privileges, and obtained this information. This has led to monetary damages when a third party uses access services without authorization, or signs up to optional services such as VoIP fraudulently.

■ Configuration Changes Caused by Malware on an Infected Home PC

There have been incidents in which an attack was launched on the configuration interface of a home router by a malware infected PC used at home, leading to DNS and other settings being changed without authorization. For example, the DNS Changer malware*63 that was paralyzed in 2012 not only changed the DNS settings on an infected PC, but also contained attack code that attempted to change settings on home routers.

■ DNS Open Resolver Participation in DDoS Attacks

Some home routers are at risk of having their functions used from external locations under the default settings. In particular, functions for assisting DNS name resolution so that devices connected to a home network can communicate over the Internet can play a part in amplifying the volume of traffic when they are exploited from the Internet (Figure 14). Even though

*58 See the following CloudFlare blog post for more information about this attack. "The DDoS That Almost Broke the Internet" (http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet).

*59 In this report, home routers refer to devices that function as terminating equipment for services such as cable TV Internet connections and DSL connections. This is also commonly called Customer Premises Equipment (CPE) by providers.

*60 In light of this attack, the Open Resolver Project (http://openresolverproject.org/), which surveys IP addresses around the world to identify addresses with settings that could be used in DNS amplification attacks, issued an alert urging users to review the settings of CPE devices such as home routers.

*61 More information about this incident can be found in the following presentation by Brazilian CSIRT organization CERT.br. (http://www.cert.br/docs/palestras/certbr-firstsymposium2012.pdf). We also reported further details in the following IIJ-SECT blog post. "Home Routers Reference Fake DNS Server due to Unauthorized Configuration Changes" (https://sect.iij.ad.jp/d/2012/06/148528.html).

*62 For example, the following domestic product. Telecom-isac Japan, "[Warning] Logitec Brand Router Vulnerability, and Steps to be Taken by Users" (https://www.telecom-isac.jp/news/news20120730.html) (in Japanese).

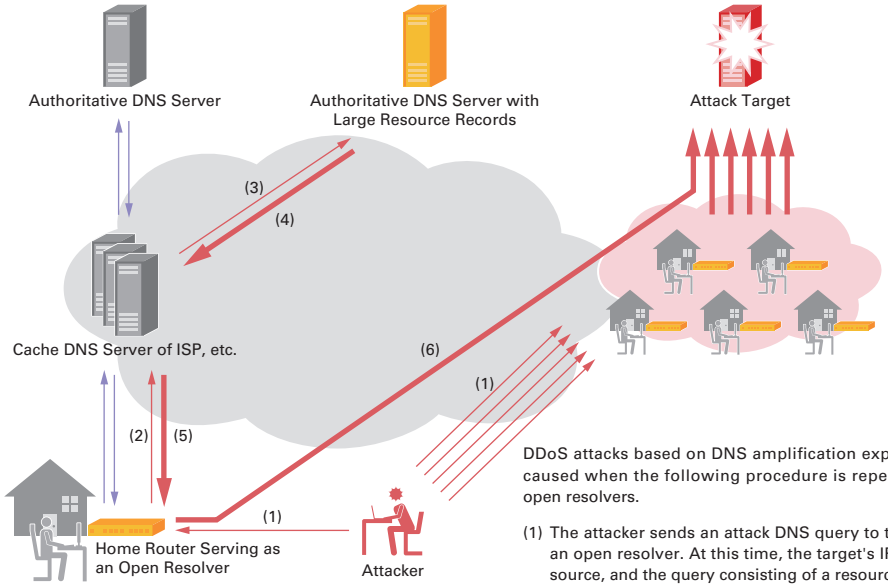
*63 See "1.4.2 DNS Changer Malware" in IIR Vol.15 (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol15_EN.pdf) for more information about the DNS Changer malware. Additionally, the following incident in Mexico in 2012 is an example in which users accessing individual servers for banks were redirected to a malicious site. Trend Micro, "Targeted Attack in Mexico: DNS Poisoning via Modems" (http://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attack-in-mexico-dns-poisoning-via-modems/).

individual home routers can only amplify traffic by a small amount, when a large number of Internet-connected devices are exploited in the same way, they can cause a large-scale DDoS attack such as the example in Europe presented above. In a statement from CloudFlare regarding another attack*64, open resolvers in a large number of countries served as stepping stones, with 4,625 IP addresses in Japan also having a hand in the incident*65.

Attacks using this method have also taken place in the past, but recently it has been used in particularly large-scale attacks, such as one that peaked at 167 Gbps in May*66. IIJ's MITF honeypot observations also show that attempts to set off these attacks are carried out on a daily basis.

Vulnerabilities in Libupnp

It is clear that vulnerabilities related to the Universal Plug and Play library that were disclosed in January 2013*67 affect some home routers*68. Unless firmware that eliminates the vulnerabilities is used, there is a risk of users being left open to attacks from the Internet*69.



Under normal DNS name resolution, shown by the purple lines, the home network device sends DNS queries to the home router, and the home router forwards these to the external cache DNS server of the ISP, etc. The DNS server of the ISP ultimately sends queries to an authoritative DNS server on the Internet, and the resource records corresponding to the query are acquired in response. This response is forwarded to the home router, and the home router passes it on to the device that issued the query.

DDoS attacks based on DNS amplification exploiting open resolvers are caused when the following procedure is repeated for large numbers of open resolvers.

(1) The attacker sends an attack DNS query to the home router serving as an open resolver. At this time, the target's IP address is spoofed as the source, and the query consisting of a resource record containing a large amount of information is requested.
(2) The home router processes the DNS query from the attacker as if it were a request from the home network, and forwards it to the DNS server of the ISP, etc.
(3) Because these communications are from a legitimate user, the DNS server of the ISP cannot differentiate between the attack DNS query and legitimate DNS queries, so it sends the attack DNS query to the Internet-based authoritative DNS server.
(4) Based on the content of the attack DNS query, large resource records are sent from the authoritative DNS server to the ISP's DNS server as the attack response.
(5) The ISP's DNS server forwards the attack response to the home router.
(6) The home router forwards the attack response it receives to the source. In this case, the source is the IP address of the target spoofed by the attacker.

Figure 14: DNS Amplification DDoS Attacks using DNS Open Resolvers as Stepping Stones

*64 According to CloudFlare's "The curse of the Open Recursor" (http://www.apricot2013.net/__data/assets/pdf_file/0009/58878/tom-paseka_1361839564.pdf) presentation at Apricot 2013, Japan account for the most IP addresses in the Asia-Pacific region for the attack example introduced.
*65 However, the same presentation indicated many of the open resolvers that played a part in the attack were servers, and it is not known to what degree home routers contributed to the attack as a whole.
*66 See the following Prolexic announcement for more information on this attack. "Prolexic Stops Largest-Ever DNS Reflection DDoS Attack" (http://www.prolexic.com/news-events-pr-prolexic-stops-largest-ever-dns-reflection-ddos-attack-167-gbps.html).
*67 The following Rapid7 report contains information on a number of vulnerabilities. "Portable SDK for UPnP Devices (libupnp) contains multiple buffer overflows in SSDP" (http://www.kb.cert.org/vuls/id/922681).
*68 The following JVN summarizes information on the products affected by the multiple vulnerabilities identified. JVN, "JVNVU#90348117 Buffer overflow vulnerabilities in Portable SDK for UPnP" (https://jvn.jp/cert/JVNVU90348117/index.html) (in Japanese).
*69 At the time of writing, the results of a search using SHODAN (http://www.shodanhq.com/), which collects information on implementations by IP address, showed 28 million IP addresses worldwide (approximately 2.7 million in Japan) that respond to the SSDP protocol used in initial UPnP negotiation. However, this figure is thought to include devices such as printers connected to networks run under a comparatively open policy, like those at universities, so it does not only represent home routers.

■ Security Risks on Vulnerable Home Routers

Leaving a home router in a vulnerable state generates different risks in terms of the following three perspectives.

Risks Regarding Personal Privacy

Home routers are key devices on a home network, and may expose details of household Internet usage. There is also a risk of direct invasion of privacy when vulnerabilities in network-enabled home electronics are exploited using a home router as a stepping stone, allowing your household to be viewed by anyone*70.

Risks for Companies and Organizations

The portable information and communication equipment (smartphones and tablets, etc.) that has seen explosive growth in use recently poses an indirect risk to companies and organizations. In particular, when the use of personal devices for work is allowed, such as in BYOD schemes, it is questionable whether it is wise to trust smartphones that are connected to compromised home environments on a daily basis to access work information. Additionally, communications from a home network environment are mostly from family, and those on the receiving end tend to trust this unconditionally. This presents the risk of communications being applied in targeted attacks, etc.

Risks for the Internet as a Whole

Because there are a vast number of home routers, they can cause attacks that are severe in overall scale even though individually they only generate a small amount of traffic when exploited. Most home routers also have few features for recording communications, and the fact they can be used as stepping stones to make it harder to trace the true attacker is a serious issue.

From these assumptions, we believe leaving the situation as it is would be extremely dangerous from a number of perspectives, and we think corrective measures should be taken urgently.

■ Fact-Finding Survey on Vulnerable Home Routers in Japan

Few of the overseas surveys presented above provide precise information indicating the current status in Japan, so Telecom-ISAC Japan*71, a security organization made up of a gathering of domestic telecom carriers, is conducting a fact-finding survey on the situation here*72. This survey focuses on ascertaining whether the management interface of a home router can be accessed, whether or not it responds to protocols related to Universal Plug and Play, and whether or not there are factors that increase the volume of DNS communications such as DNS open resolvers. The application of a unique survey environment is aimed at ascertaining the status with highly reliable and accurate figures.

At the time of writing, no statement has been made regarding the publishing of results from the survey, but if the situation is particularly serious, they will be used to evaluate countermeasures for resolving the issues.

■ Resolving the Situation

As of now, we can envisage two approaches to resolving this situation. One is to bring the technology and techniques used for the secure operation of networks at organizations such as corporations into home networks, and use them for everyday operation. Another is to regulate communications on the Internet side to reduce risks.

To run a home network in the same way as a corporate one, users must first identify all the devices that will connect to it, make note of the vulnerability information for each of them, and endeavor to use the latest firmware. Then, it is necessary to confirm the security of settings, and check a daily communications log. This would require an inordinate amount of work, meaning that tools for assisting these processes would be essential for implementing them in day-to-day life.

The product developers that provide home routers would also need to aim to make their products more secure. For example, they should provide default settings that can be used safely by simply turning on the power when deploying a device, and

*70 A vulnerability that enables control of the camera function in South Korean Samsung brand network-enabled TVs has actually been reported. Sophos Nakedsecurity Blog, "Samsung Smart TV security hole allows hackers to watch you, change channels or plug in malware" (http://nakedsecurity.sophos.com/2012/12/12/samsung-tv-vulnerability/).

*71 Telecom Information Sharing and Analysis Center Japan (https://www.telecom-isac.jp/english/index.html).

*72 Telecom-ISAC Japan, "A Survey on the Presence of Vulnerabilities in Network Devices" (https://www.telecom-isac.jp/news/news20130617.html) (in Japanese).

design a system for responding quickly to vulnerabilities, publicizing new firmware, and distributing fixes appropriately through functions such as auto updates. The addition of a function for detecting external use would also be necessary. Furthermore, improved functions for recording summaries of communications would be required to protect the devices connected to home networks.

Telecom carriers and security providers must look into services for checking configuration issues, and managing the operation of home routers over the Internet. It would also be worth considering widespread implementation of walled garden*73 access services, which have functions for protecting the communications devices of users.

Meanwhile, the regulation of communications could result in lost opportunities and adverse effects*74, and would need to be evaluated carefully. The regulation of communications should be discussed as a realistic countermeasure only when it became clear that the situation could not be corrected through the individual efforts of product developers or ISPs, such as if several million home routers were discovered to have vulnerabilities in a fact-finding survey, for example.

The implementation of measures such as those considered here would take a significant amount of time. As for measures that can be initiated immediately, a number of security organizations, Internet-related organizations, and ISPs have begun efforts to encourage general users to use functions on their current routers and confirm their soundness.

1.4.3 A Spate of Unauthorized Login Incidents

From around March 2013, there was a spate of unauthorized login (fraudulent login)*75 incidents targeting registration-based online services in Japan, and unauthorized access incidents thought to be aimed at the theft of registration information. In this report we present an overview of this series of incidents, and propose measures that users can implement.

■ Unauthorized Login Techniques

Generally one of the following three techniques are used in large-scale unauthorized logins*76. The most basic attacks involve brute force attempts to find valid strings for the ID and password (“aaaa,” “aaab,” “aaac”...), in what are called brute force attacks. A more efficient attack technique is the dictionary attack, in which a dictionary of commonly-used strings

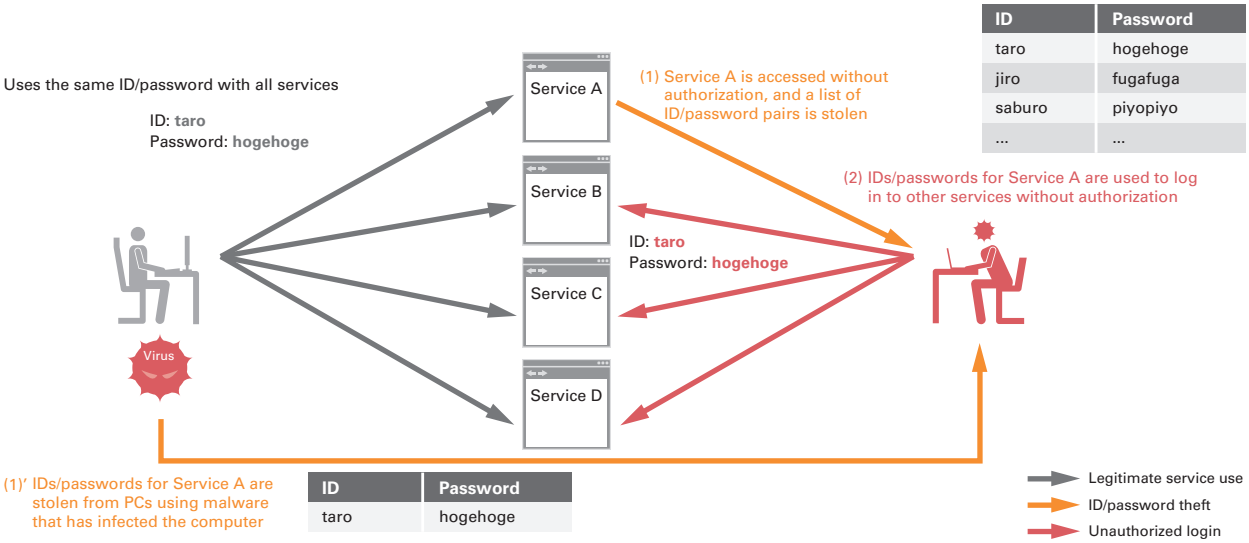


Figure 15: Illustration of List-Based Unauthorized Login

*73 See the following MAAWG reference material for more information on walled gardens at ISPs. “MAAWG BEST PRACTICES FOR THE USE OF A WALLED GARDEN” (http://www.maawg.org/sites/maawg/files/news/MAAWG_Walled_Garden_BP_2007-09.pdf).

*74 The adverse effects mentioned here refer to the Internet not allowing communications to be carried out at the desired time. For example, if Universal Plug and Play were not usable over the Internet, the anticipated impact would be minor. However, depending on the approach, regulation of HTTP used in Web management interfaces or DNS communications could create a situation very different from the Internet we know today. For example, it may be significantly more difficult to build your own server at home.

*75 In this report, with regard to a given online service that requires authentication, we refer to service login by a third party without the original ID owner’s intent as “unauthorized login.”

*76 For small-scale unauthorized login, such as incidents conducted manually by an acquaintance of the target, etc., common methods used include guessing the password based on profiles, and social engineering to get the other party to reveal their password through trickery.

("password," "abc123," etc.) is prepared, and each entry attempted one-by-one. Finally, the list-based attack technique involves login attempts using lists of ID and password combinations obtained by the attacker in advance. Attackers are believed to create these lists from account information stolen through unauthorized access to other online services, account information gathered via phishing, and account information stolen directly from users' PCs using malware*77 (Figure 15).

Normally, list-based attacks are not a large issue as long as different IDs and passwords are used for each online service. However, in an awareness survey conducted by IPA in 2012, just 20% of respondents answered that they set different passwords for each service*78. In light of this, list-based attacks can be a very effective technique.

When unauthorized login succeeds, it is difficult for the service provider to determine whether a party is the original user or not, so depending on the details provided by the service, attackers are free to view personal information, purchase goods, or transfer valuables at will. A number of publicly-disclosed incidents actually involved attackers logging into online shopping sites that provide a points service without authorization, and using points fraudulently.

■ The Series of Attacks and their Purpose

Table 1 summarizes the main incidents of unauthorized login and unauthorized access disclosed in 2013. Focusing on unauthorized login, we can see that online services in the same industries, such as communication-related services or e-commerce services, have been attacked within a short space of time. This suggests that the corresponding attacks were carried out by the same attacker, or by parties with some kind of connection. Assuming this kind of attack group is involved, and reflecting on the spate of unauthorized login incidents targeting Japan-oriented services since the beginning of this year, we can surmise that highly effective dictionaries and lists combining the user IDs and passwords of Japanese users are becoming readily available to attacker communities, etc.

Table 1: Major Account Leaks due to Unauthorized Login and Unauthorized Access Disclosed in 2013

Disclosure Date	Service Type		Period	Incident Type	No. of Unauthorized Logins / Leaked Accounts	Notes
April 3	Search portal	Company A	April 1 to April 9	Unauthorized login attempts	108,716	
April 4	Communications-related service	Company B	April 4	Unauthorized login attempts	30	
April 4	Search portal	Company C	Until April 2	Unauthorized access	0	1.27 million sets of account information were collected on the server, but did not leak
April 5	Point-related service	Company D	March 26	Unauthorized login attempts	299	Points were used fraudulently
April 6	E-book service	Company E	April 2 to April 5	Unauthorized login attempts	779	Credit card information may have leaked
April 10	Communications-related service	Company B	April 9 to April 10	Unauthorized login attempts	77	
April 17	Transit service	Company F	March 31	Unauthorized login attempts	97	
April 22	Payment service	Company G	April 18 to April 19	Unauthorized login attempts	5,450	
May 8	E-commerce service	Company H	May 4 to May 8	Unauthorized login attempts	Approximately 15,000	
May 17	Beauty service	Company I	May 6 to May 12	Unauthorized login attempts	682	
May 17	Search portal	Company C	Until May 16	Unauthorized access	1,486,000	Up to 22 million sets of account information were collected on the server, but of these only 1,486,000 may have leaked
May 25	E-commerce service	Company J	May 6 to May 23	Unauthorized login attempts	8,289	
May 29	E-commerce service	Company K	Until May 13	Unauthorized login attempts	2,382	Credit card information may have leaked
June 3	E-commerce service	Company L	April 24 to May 31	Unauthorized login attempts	9,609 (up to 16,808)	Credit card information may have leaked
June 19	E-commerce service	Company M	June 18	Unauthorized login attempts	126	
July 5	Game related	Company N	June 9 to July 4	Unauthorized login attempts	23,926	
July 9	Game related	Company O	June 13 to July 7	Unauthorized login attempts	35,252	
July 10	E-commerce service	Company P	May 10 to July 8	Unauthorized login attempts	—	Points were used fraudulently
July 17	Communications-related service	Company Q	July 14 to July 16	Unauthorized login attempts	21,184	
July 19	News portal	Company R	July 17 to July 18	Unauthorized access	1,692,496	Attacker was identified and the leaked information confirmed to be deleted
July 24	Communications-related service	Company S	Up to July 23, July 26	Unauthorized access	Up to 4,000,000	
July 26	Point-related service	Company D	July 15	Unauthorized login attempts	27	Points were used fraudulently
August 8	Social content	Company T	July 25 to August 5	Unauthorized login attempts	39,590	
August 8	Travel service	Company U	February 14 to February 16, June 3 to June 15	Unauthorized login attempts	27,620	
August 12	Social content	Company V	April 6 to August 3	Unauthorized login attempts	243,266	

*The information in the table is based on details published by affected service providers.

*77 In the Gumblar attacks, which had a significant impact on the Web environment in Japan in 2009, FTP account information stored on PCs was stolen by malware that spread via drive-by download, and this account information used repeatedly in new website alteration incidents. See "ID/Password Stealing Gumblar Malware" in Vol.4 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol04_EN.pdf) for more information.

*78 IPA, "Survey on Awareness of Information Security Threats for FY2012" (http://www.ipa.go.jp/security/fy24/reports/ishiki/) (in Japanese).

The account information stolen through the incidents of unauthorized access listed in Table 1 may also have been exploited right away in unauthorized login attempts (list-based attacks and dictionary attacks*79).

Meanwhile, the intentions of the attackers behind this series of unauthorized logins are not known. Excluding three cases in which points were used fraudulently with certain shopping services and point exchange services, this series of unauthorized login incidents caused no damages other than the act of logging in itself. For several incidents, it is stated that credit card information may have been leaked. However, this merely indicates that credit card information could have been viewed, and as of August 2013, there have been no reports of damages due to the fraudulent use of leaked credit card information.

For this reason, it appears that attackers are simply checking that the ID and password combination tested works with the target online service.

Furthermore, according to information disclosed in several cases, the attackers' behavior seems to suggest they are not worried about the attacks being detected, with a large number of unauthorized login attempts from a small number of attack sources repeated in a comparatively short space of time. When attacks are exposed, providers of online services can request that users change their password. This means the attackers haven't considered that their behavior could lead to the valid ID and password combination they have gone to the trouble of confirming being changed.

It is difficult to guess whether there is some hidden agenda behind the manner in which the attacks were made, or whether the attackers simply do not care. In any case, we must stay vigilant and prepare for more refined attacks in the future.

■ Unauthorized Login Countermeasures on the Service Provider Side

The fundamental measures against unauthorized login that service providers should consider include the following.

(1) Use a password that is as complex and long as possible
(2) Tell users to use different passwords for each service
(3) Provide two step / multifactor authentication
(4) Provide a way to confirm login history and purchase procedures
(5) Detect and protect against unauthorized login attempts

Policies similar to (1) and (2) were repeatedly recommended by online service providers in around 2008*80. For (1) in particular, service providers should consider prohibiting the registration of passwords that are too short, not complex enough (in the character types used), or that contain phrases commonly found in the dictionary.

Support for (3) can effectively prevent unauthorized login via list-based attacks, such as those occurring now. Multifactor authentication using hardware tokens is already provided for some financial services. Additionally, many portal sites and SNS have added support for two step authentication since the beginning of the year.

We recommend that (4) is also implemented in case damage has been caused, or for when you want to confirm that no damage has been inflicted. It is important that users who have been directly affected by unauthorized logins are able to confirm whether or not they have suffered damages.

Item (5) refers to systems for reporting on and blocking suspicious behavior by setting a threshold for the number of login attempts per unit of time, and the number of simultaneous logins, on a per account and source IP address basis. It is necessary to consider the items to monitor, their thresholds, and the response to take when suspicious behavior is detected, based on the nature of the service provided.

*79 In addition to list-based attacks that use pairs of stolen IDs and passwords as-is, when plain text passwords cannot be obtained, dictionary attacks using lists of IDs obtained and dictionaries of typical passwords may be carried out.

*80 NIFTY Corporation, "Stop Using the Same Passwords!" (http://support.nifty.com/support/information/1114_pass.htm) (in Japanese), Rakuten, "Take Care when Managing Rakuten User IDs and Passwords" (http://www.rakuten.co.jp/com/faq/information/20081029.html) (in Japanese), Yahoo! JAPAN, "Use Different Passwords for each Site!" (http://security.yahoo.co.jp/attention/password/) (in Japanese).

Furthermore, as demonstrated by the recent incidents, servers are often overloaded by large-scale attack attempts, so in some cases unauthorized login attempts are discovered through resource monitoring.

■ Countermeasures for Unauthorized Login on the User Side

User-side countermeasures involve actively utilizing the functions provided by service providers, and in particular items (1) through (4) mentioned above. For (1), users do not need to come up with their own ideas, as ideally they should create a complex password using a password generation tool. Use of a password management tool is an effective way to keep complex passwords together, and achieve (2) without undue strain.

It should also be noted that even when implementing the use of advanced passwords such as this, it is still not possible to completely eliminate the risk of unauthorized login through the theft of passwords or security tokens using refined phishing and social engineering techniques, and advanced malware.

From a user's perspective, it is desirable to periodically check (4) with regard to financial services and shopping services of particular importance, in the interest of self-preservation.

1.5 Conclusion

This report has provided a summary of security incidents to which IIJ has responded. This time we discussed techniques for detecting ZeroAccess malware, examined the impact of vulnerable home routers, and looked into a spate of unauthorized login incidents. IIJ makes every effort to inform the public about the dangers of Internet usage by identifying and publicizing incidents and associated responses in reports such as this. IIJ will continue striving to provide the necessary countermeasures to allow the safe and secure use of the Internet.

Authors:

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

Hirohide Tsuchiya (1.2 Incident Summary)
Hirohide Tsuchiya, Hiroshi Suzuki (1.3 Incident Survey)
Takahiro Haruyama (1.4.1 An Examination of ZeroAccess and its IOC)
Mamoru Saito (1.4.2 Home Router Security)
Hisao Nashiwa (1.4.3 A Spate of Unauthorized Login Incidents)
Office of Emergency Response and Clearinghouse for Security Information, Service Operation Division, IIJ

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