The PlugX RAT Used in Targeted Attacks

In this report, we discuss the PlugX RAT used in targeted attacks, and look at examples of the continuing targeted email attacks and their countermeasures. We also examine the Bitcoin virtual currency that has begun to take hold as a new form of currency among some Internet users.

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. In the period covered by this volume, from July 1 to September 30, 2013, large-scale attacks were expected in relation to historic dates of the Pacific War. However, aside from damage incurred from some incidents such as website alterations, as a whole most attacks were only small in scale. That said, there were a number of attacks linked to hacktivism by Anonymous and other groups. There were also a series of Web server compromises and related website alterations and information leaks. Attacks on domain registries including ccTLD continue to occur, along with associated domain hijackings and information leaks. Probing for DNS open resolvers and DDoS attacks exploiting them were also confirmed. As seen above, the Internet continues to experience many security-related incidents.

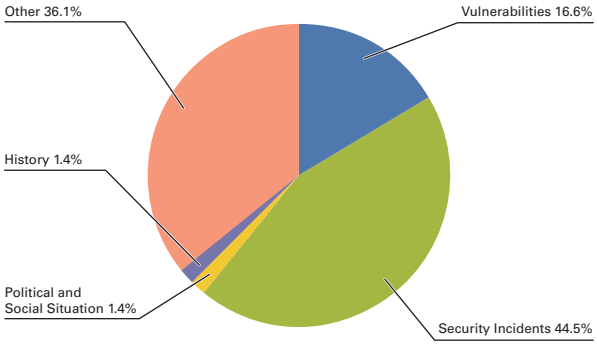


Figure 1: Incident Ratio by Category (July 1 to September 30, 2013)

1.2 Incident Summary

Here, we discuss the IIJ handling and response to incidents that occurred between July 1 and September 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. Major incidents included account information and internal data leaks due to a number of attacks on websites related to the government of the United States, such as the leak of email addresses and passwords for those involved with U.S. Congress, and information leaks from the Federal Emergency Management Agency (FEMA) (OpLastResort). In August, there were many attacks on websites related to the governments of Pakistan and India around the anniversary of their independence*2.

*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.

*2 See the following Hackmageddon.com article for a summary of these attacks. "Timeline of Cyber Attacks in Conjunction with the Pakistan and India Independence Days" (http://hackmageddon.com/2013/08/22/timeline-of-cyber-attacks-in-conjunction-with-the-pakistan-and-india-independence-days/).

These attacks were not limited to the websites of government institutions, as they also spread to sites such as an external SNS service related to the government, including alterations to a Facebook page for the Pakistan military.

In September, attacks on sites related to the governments of mainly South American countries continued to occur, perpetrated by members of Anonymous in each country. Additionally, there are ongoing attacks on sites related to the Turkish government agencies, thought to be carried out by the Syrian Electronic Army. Groups other than Anonymous also continue to be active, as demonstrated by phase four in a series of DDoS attacks on U.S. financial institutions that resumed in July (Operation Ababil).

■ Vulnerabilities and their Handling

During this period fixes were released for Microsoft's Windows*3*4, Internet Explorer*5*6*7, and Office*8*9. Updates were also made to Adobe Systems' Flash Player, Reader, Acrobat, and Shockwave Player. Oracle released a number of updates for Java that fixed many vulnerabilities. Several of these vulnerabilities were exploited before patches were released.

Many vulnerabilities were also fixed in server applications, including a number in Microsoft's SharePoint Server*10 that could allow arbitrary code exception when specially crafted packets were received from a remote source. A quarterly update was also released for Oracle, fixing a large number of vulnerabilities. A vulnerability in BIND9 DNS server that caused abnormal server stoppages through the processing of specially crafted requests was also fixed.

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. IPA issued a warning due to the large number of alterations involving websites using CMS applications that had not been updated, including the exploitation of the above vulnerabilities*11.

■ Attacks Based on Political and Social Situation and Historical Context

During this period each year there are incidents related to historical dates in the Pacific War, as well as Takeshima and the Senkaku Islands. We stayed vigilant, as this year attack warnings and other information once again led to expectations that the websites of a number government agencies and private-sector businesses in Japan would be subject to alterations through compromise via SQL injections and brute force attacks, as well as DDoS attacks, in relation to these sensitive issues. However, although some website alterations were noted in news reports, no large-scale attacks were confirmed.

IIJ observed a UDP and SYN flooding DDoS attack on September 17 that peaked at just under 3 Gbps, and confirmed a number of large-scale attacks that lasted a comparatively short time. DDoS attacks were also more prevalent than usual around September 18. However, the scale and number of attacks were much lower than for the same period last year.

It is not clear why there were fewer large-scale synchronized attacks than usual, but we believe it may be because no major incidents that could trigger attacks occurred between Japan and neighboring countries, unlike circumstances during this period in 2010 or 2012.

---

*3 "Microsoft Security Bulletin MS12-053 - Critical: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2850851)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-053).

*4 "Microsoft Security Bulletin MS13-060 - Critical: Vulnerability in Unicode Scripts Processor Could Allow Remote Code Execution (2850869)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-060).

*5 "Microsoft Security Bulletin MS13-055 - Critical: Cumulative Security Update for Internet Explorer (2846071)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-055).

*6 "Microsoft Security Bulletin MS13-059 - Critical: Cumulative Security Update for Internet Explorer (2862772)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-059).

*7 "Microsoft Security Bulletin MS13-069 - Critical: Cumulative Security Update for Internet Explorer (2870699)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-069).

*8 "Microsoft Security Bulletin MS13-054 - Critical: Vulnerability in GDI+ Could Allow Remote Code Execution (2848295)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-054).

*9 "Microsoft Security Bulletin MS13-068 - Critical: Vulnerability in Microsoft Outlook Could Allow Remote Code Execution (2756473)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-068).

*10 "Microsoft Security Bulletin MS13-067 - Critical: Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (2834052)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-067).

*11 IPA, "A Warning to Websites Using Old Versions of WordPress or Movable Type" (http://www.ipa.go.jp/security/topics/alert20130913.html) "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).

July Incidents

1 S **1st:** In South Korea, there were attacks following on from those on June 25 in which a number of websites were altered, including the sites of media-related companies.
See the following nProtect blog post for more information about this incident. "[긴급]6.25 사이버전, 국내 주요 사이트 해킹 공격 받는 중 Update # 130701-21" (http://erteam.nprotect.com/429) (in Korean)

2 S **1st:** The MYNIC registry for Malaysia's .my domains was accessed by an unknown entity without authorization, and a number of well-known domains including those for Microsoft and Dell were hijacked.
See the following MYNIC announcement for more information about this incident. ".my DOMAIN NAME INCIDENT RESOLVED" (http://mynic.my/en/news.php?id=155).

5 S **2nd:** Japan Aerospace Exploration Agency (JAXA) published the results of an investigation into unauthorized access that occurred in April.
Japan Aerospace Exploration Agency "Regarding the Results of an Investigation Into Unauthorized Access of JAXA Server" (http://www.jaxa.jp/press/2013/07/20130702_security_j.html) (in Japanese).

7 S **3rd:** Researchers reported that personal information was being collected from Motorola mobile devices without the users' intention. This report indicated that personal information, including account information for external Web services, was being sent to a domain host related to Motorola.
See the following blog post from Ben Lincoln, who discovered the issue, for more information. Beneath the Waves, "Motorola Is Listening" (http://www.beneaththewaves.net/Projects/Motorola_Is_Listening.html).

9 V **4th:** A vulnerability in the signatures used on Android to determine whether or not an application is legitimate was disclosed, and it was reported that this affected a large number of devices. The details of this vulnerability were made public at the Black Hat USA 2013 conference held in August.
See the following presentation made by Jeff Forristal at Black Hat USA 2013 for more information. Android: One Root to Own Them All (https://media.blackhat.com/us-13/US-13-Forristal-Android-One-Root-to-Own-Them-All-Slides.pdf).

11 O **4th:** The Council on ICT Strategy and Policy for Growth of the Ministry of Internal Affairs and Communications officially announced its ICT Strategy and Policy for Growth, which summarized important points for applying ICT to the growth of the economy and contributing to the international community.
"Official Announcement of ICT Strategy and Policy for Growth" (http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/130704_05.html).

14 S **9th:** Content on Web servers of the DNS Belgium (.be) domain registry were altered by an unknown entity. Registered DNS information was apparently not affected by this incident.
See the following announcement from DNS Belgium for more information. "Deface hack on DNS.be website" (http://www.dns.be/en/news/recent_news/deface-hack-on-dnsbe-website2#.UIyiaVBzPkc).

16 S **9th:** The SIDN domain registry for the Netherlands (.nl) announced it had suspended a number of services after being accessed without authorization through an SQL injection attack. It also reset all registrar passwords as a preventive measure.

17 V **10th:** Microsoft published their Security Bulletin Summary for July 2013, and released six critical updates including MS13-053 and MS13-055, as well as one important update.
"Microsoft Security Bulletin Summary for July 2013" (http://technet.microsoft.com/en-us/security/bulletin/ms13-jul).

18 V **10th:** A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB13-17: Security updates available for Adobe Flash Player" (http://www.adobe.com/support/security/bulletins/apsb13-17.html).

20 O **11th:** The JPCERT Coordination Center published a report on responses to incident reports between April and June 2013. There were an extremely large number of reports of websites thought to have been altered by inserting suspicious iframes or obfuscated JavaScript into pages.
"JPCERT/CC Incident Report Response Report [April 1, 2013 to June 30, 2013]" (http://www.jpcert.or.jp/pr/2013/IR_Report20130711.pdf) (in Japanese).

22 V **17th:** Oracle released their quarterly scheduled update for a number of products including Oracle, fixing a total of 89 vulnerabilities.
"Oracle Critical Patch Update Advisory - July 2013" (http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html).

23 V **17th:** A number of vulnerabilities in Apache Struts were discovered and fixed, including one that allowed remote execution of arbitrary OS commands by third parties (CVE-2013-2251).
See the following JPCERT Coordination Center alert for more information. "JPCERT/CC Alert 2013-07-19 Vulnerability in Apache Struts (S2-016)" (http://www.jpcert.or.jp/english/at/2013/at130033.html).

25 S **17th:** U.S. company Network Solutions was targeted by a large-scale DDoS attack, which prevented user pages from being viewed.
See the following Network Solutions announcement for more information about this incident. "A Note to Our Customers" (https://www.networksolutions.com/blog/2013/07/a-note-to-our-customers/?channelid=P99C425S627N0B142A1D38E0000V100).

26 S **19th:** GitHub was targeted by a large-scale DDoS attack that caused a service outage.
See the following GitHub Status overview for more information about this incident. "Status Messages" (https://status.github.com/messages/2013-07-19).

28 V **27th:** A vulnerability in all versions of BIND 9.7 that could cause service outages through specially crafted queries containing improper RDATA was discovered and fixed. Because BIND 9.7 had already reached EOL status, an update to a version in which this vulnerability was fixed (BIND 9.8.5-P2/9.9.3-P2) was recommended.
Internet Systems Consortium, "CVE-2013-4854: A specially crafted query can cause BIND to terminate abnormally" (https://kb.isc.org/article/AA-01015).

31 S **28th:** Content on Web servers of the DNS Belgium (.be) domain registry were once again altered by an unknown entity.
See the following announcement from DNS Belgium for more information. "A detailed account of the hack on DNS.be" (http://www.dns.be/en/news/recent_news/a-detailed-account-of-the-hack-on-dnsbe#.UI0wxFBzPkc).

[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

Since around March of this year, there has been an outbreak of attempts to log in through identity fraud in which it is believed lists of IDs and passwords were used, along with attempts to steal the IDs and passwords of users. In this survey period these attempts continued to occur*12.

During this period, there were many incidents of unauthorized login attempts on a large number of websites, including member-oriented service sites such as e-commerce sites and mobile social networking sites, as well as member sites for companies related to games or travel. In many of these incidents, there is a possibility that registered information was viewed following unauthorized login, and in some cases points were used without authorization.

Regarding incidents in which IDs and passwords were targeted, it was announced that for some incidents of unauthorized access at a number of SNS sites, the culprits were identified through cooperation with foreign police, and the data acquired without authorization was deleted after confirming that it had not been leaked to third parties.

In some of these incidents vulnerabilities and other methods were used to compromise servers, and in addition to the leak of member information, the websites were altered and used in other incidents such as phishing or the sending of spam. This demonstrates that we must continue to remain cautious.

■ DNS Open Resolver Communications

During the current survey period, a number of probing attempts and attacks on DNS open resolvers were confirmed. Regarding DNS amplification DDoS attacks using DNS open resolvers as stepping stones, this March the large-scale DDoS attack on the Spamhaus anti-spam organization generated a lot of interest, and IIJ also noted an DNS amplification DDoS attack that peaked at 3 Gbps, as well as a number of similar incidents following on after it.

In September, the National Police Agency issued an alert due to a rise in access to 53/UDP originating from China*13. Figure 2 shows the IP addresses for senders of 53/UDP communications coming into our honeypots classified by country. As this indicates, there was an extremely large amount of communications originating from China after September 10. After examining these communications, it appears they were name resolution attempts for multiple domain names originating from a number of specific IP addresses. Because the domain names used in queries from these communications were designed to return responses containing a large volume of information, they are believed to be domains prepared in advance for an attack. However, the total volume of communications per honeypot confirmed during this period was not that large, and it was not clear whether the sources of these communications were scanning for open resolvers, or being targeted by a DNS amplification DDoS attack. Similar communications were also confirmed on overseas honeypots, so we think there is little chance they involved an intentional attack on Japan. Additionally, as a result of this survey, we have confirmed that a small number of attempts to scan for DNS open resolvers originating in China have been carried out regularly since at least

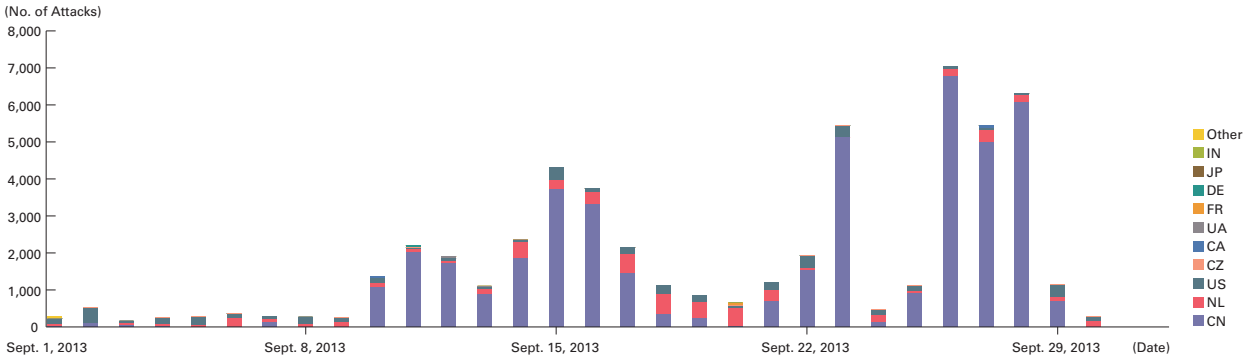


Figure 2: 53/UDP Communications Arriving at Honeypots (by Date, by Country)

*12 See "1.2 Incident Summary" from IIR Vol.20 (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol20_EN.pdf) for more information about the circumstances for the period from April to June.

*13 National Police Agency, "A rise in scanning behavior for DNS servers that allow recursive queries originating from China" (http://www.npa.go.jp/cyberpolice/detect/pdf/20130911.pdf) (in Japanese).

August Incidents

1 **1st:** At Black Hat USA 2013, a German security researcher announced that 56-bit DES was used in some SIM cards, and there was a vulnerability that could lead to a SIM card's encryption key leaking through a specially crafted SMS.
See the following Black Hat USA 2013 presentation for more information. "ROOTING SIM CARDS" (http://www.blackhat.com/us-13/archives.html#NohI).

2 **1st:** Twitter published its Transparency Report for the first half of 2013, which summarized the number of requests from each countries' government, etc., for the disclosure or deletion of information.
Twitter, Inc., "Transparency Report" (https://transparency.twitter.com/).

3 **2nd:** A new BREACH attack method on SSL/TLS was announced at Black Hat USA 2013.
See the BreachAttack.com site (http://breachattack.com/), which contains an explanation from the presenters, for more information.

4 **2nd:** A vulnerability was disclosed in the Open Shortest Path First (OSPF) protocol specification that could allow routing table contents to be altered due to an issue with the identification of router Link State Advertisements (LSAs).
US-CERT, "Vulnerability Note VU#229804 Open Shortest Path First (OSPF) Protocol does not specify unique LSA lookup identifiers" (http://www.kb.cert.org/vuls/id/229804).

5 **2nd:** LINE Corporation announced that together with overseas local police it had identified the person who had accessed a number of the services it operates without authorization on July 19, and deleted the data that they had acquired. It also confirmed that there were no traces to suggest access by unauthorized login, alteration of data, or the leak of information to third parties had been carried out.
See the following LINE Corporation press release for more information. "[NAVER] Notice regarding unauthorized access to NAVER member information (follow-up)" (http://linecorp.com/press/2013/0802585) (in Japanese).

6 **4th:** Microsoft published an advisory about problems resulting from a known weakness in PEAP-MS-CHAPv2, which is used for WPA2 wireless authentication on Windows Phone.
"Microsoft Security Advisory (2876146) Wireless PEAP-MS-CHAPv2 Authentication Could Allow Information Disclosure" (http://technet.microsoft.com/en-us/security/advisory/2876146).

7 **5th:** A service provider of Tor hidden services attracted interest when malicious code using a known vulnerability in Firefox that was fixed in June was discovered.
See the following The Tor Blog post for more information. "Hidden Services, Current Events, and Freedom Hosting" (https://blog.torproject.org/category/tags/freedom-hosting).

8 **5th:** An administrator's password was compromised at a domain registrar for the Netherlands (.nl), and the DNS records for a number of Web hosting companies that it managed were altered, leading to a large number of websites being redirected to malware sites.

9 **6th:** A presentation at DEF CON 21 detailed vulnerabilities in vehicle control systems.
See following materials from presenters Chris Valasek and Charlie Miller for more information. "Car Hacking: The Content" (http://blog.ioactive.com/2013/08/car-hacking-content.html).

10 **8th:** The Ministry of Internal Affairs and Communications requested that telecommunications carrier organizations cooperate in disseminating information encouraging their members' subscribers and users to implement basic anti-virus measures. This was due to a spate of unauthorized access incidents in which illegal remittances were carried out by third parties using Internet banking IDs and passwords obtained through virus infections without authorization.
"Warning Users About Reponses to Unauthorized Access Incidents Relating to Internet Banking (Request)" (http://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000076.html) (in Japanese).

11 **14th:** Microsoft published their Security Bulletin Summary for August 2013, and released three critical updates including MS13-059 and MS13-060, as well as five important updates.
"Microsoft Security Bulletin Summary for August 2013" (http://technet.microsoft.com/en-us/security/bulletin/ms13-aug).

12 **15th:** A fault that temporarily prevented the name resolution of .gov zones occurred due to DNSSEC problems.
See the following ISC Diary post for more information. ".GOV zones may not resolve due to DNSSEC problems." (https://isc.sans.edu/diary/.GOV+zones+may+not+resolve+due+to+DNSSEC+problems./16367).

13 **15th:** GitHub was targeted by a large-scale DDoS attack that caused a service outage.
See the following GitHub Status overview for more information about this incident. "Status Messages" (https://status.github.com/messages/2013-08-15).

14 **22nd:** Information Security Operation providers Group Japan (ISOG-J) held "The Situation with Non-Stop Web Alterations and Measures to Take (Private Consultations Available)," which provided an overview of Web alteration incidents in Japan as well as an opportunity for private consultation regarding specific issues.
See the following ISOG-J site for more information about the seminar. "ISOG-J Holds 'The Situation with Non-Stop Web Alterations and Measures to Take (Private Consultations Available)' Seminar" (http://isog-j.org/event/index.html) (in Japanese).

15 **25th:** A large-scale DDoS attack was made on DNS servers for China's .cn domains.
See the following CNNIC presentation for more information. CNNIC "Announcement" (http://www.cnnic.net.cn/gywm/xwzx/xwzxtzgg/201308/t20130825_41322.htm) (in Chinese).

16 **28th:** A large number of Web alterations thought to have targeted WordPress occurred at a number of hosting providers in Japan.

17 **29th:** Trend Micro issued a warning recommending an update to the latest version of Java due to confirmed attacks on an unpatched vulnerability in Java 6.
See the following TrendLabs Security Intelligence Blog post for more details. "Java 6 Zero-Day Exploit Pushes Users to Shift to Latest Java Version" (http://blog.trendmicro.com/trendlabs-security-intelligence/java-6-zero-day-exploit-pushes-users-to-shift-to-latest-java-version/).

18 **29th:** Information-technology Promotion Agency (IPA) published its "System Design Guide to Protect Against 'Targeted Email Attacks'," which gave an overall picture of targeted email attacks and their characteristics, and summarized system design-based techniques for dealing with them.
"System Design Guide to Protect Against 'Targeted Email Attacks'" (http://www.ipa.go.jp/security/vuln/newattack.html) (in Japanese).

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

*Dates are in Japan Standard Time

January of this year. These attempts were no longer observed in late August of this year, but scanning communications have been confirmed at odd intervals since then, so we believe that continued vigilance is necessary.

Attacks on TLD

Numerous attacks on domain registries including ccTLD continue to occur, along with associated domain hijackings and information leaks. In July, the MYNIC ccTLD registry that manages Malaysia's .my domains was accessed by an unknown entity without authorization, and a number of well-known domains including those for Microsoft and Dell were hijacked. The website of the DNS Belgium ccTLD registry that manages Belgium's .be domains was overwritten without authorization. Following this, DNS Belgium's website was once again compromised and Web content altered. The SIDN ccTLD registry that manages the Netherlands' .nl domains was also compromised in an SQL injection attack, and account information was reset. In the Netherlands, a ccTLD registrar was accessed without authorization, and domains were hijacked and redirected to other sites. In August, the PNINA ccTLD registry that manages Palestine's .ps domains was accessed without authorization, and sites such as Google were redirected to other sites due to domain hijackings. Also in August, there was an incident in which access to a number of media outlets and some Twitter domains was cut off due to domain hijackings after an unknown entity accessed the domain registrar used by the affected corporations without authorization*14.

Government Agency Initiatives

Government agency initiatives included the 11th assembly of the Council for Promotion of Information Security Measures (Liaison Conference for CISO, etc.). Reports were presented by a number of ministries, including those affected, regarding information leaks stemming from government agencies' use of group email services provided by private-sector businesses*15. Because access restrictions had not been properly implemented in these incidents, ministry information including confidential material had been viewable to third parties. Additionally, confirmation of multiple incidents of the use of similar services underpinned the fact that there was a need to have users thoroughly review the information security policy at each ministry. At the 12th assembly, a warning was also issued regarding the handling of ministry information that includes confidential material, as well as the use of external services*16.

In July, the Council on ICT Strategy and Policy for Growth of the Ministry of Internal Affairs and Communications officially announced its ICT Strategy and Policy for Growth, which summarized its discussions. It proposed three visions, including the creation of new value-added industry through the utilization of G-space (geographical space) information and big data. Similarly, the Ministry of Internal Affairs and Communications' Study Group on Consumer Issues with ICT Services announced its "Reinforcement Strategy on Smartphone Safety and Security," which summarized its examination of the response required to create an environment for the safe and secure use of smartphones given their associated issues. In August, due to a string of incidents of unauthorized access to Internet banking services and subsequent illegal remittances caused by PC virus infections, members of telecommunications carrier organizations were requested to cooperate in disseminating information encouraging their users to implement basic anti-virus measures. Regarding international collaborations, in September there was an ASEAN-Japan Ministerial Policy Meeting on Cyber Security Cooperation. These meetings have been conducted regularly since November last year, and this time a Joint Ministerial Statement was adopted*17.

*14 See the following Sophos Nakedsecurity Blog post for more information. "Syrian Electronic Army brings down Twitter and The New York Times through domain name provider hack" (http://nakedsecurity.sophos.com/2013/08/28/syrian-electronic-army-brings-down-twitter-and-the-new-york-times-through-domain-name-provider-hack/).

*15 National Information Security Center, "11th Assembly (July 11, 2013)" (http://www.nisc.go.jp/conference/suishin/index.html#2013_3) (in Japanese).

*16 National Information Security Center, "12th Assembly (July 30, 2013)" (http://www.nisc.go.jp/conference/suishin/index.html#2013_4) (in Japanese).

*17 National Information Security Center, "ASEAN-Japan Ministerial Policy Meeting on Cyber Security Cooperation" (http://www.nisc.go.jp/press/pdf/aseanj_meeting20130913.pdf) (in Japanese).

September Incidents

1 O **2nd:** The 1st review meeting was held by the "Investigative Commission on Personal Data," which was established by the government's IT Strategic Headquarters to conduct an inquiry into and evaluation of clarifications to rules for the use and application of personal data.
"Investigate Commission on Personal Data" (http://www.kantei.go.jp/jp/singi/it2/pd/index.html) (in Japanese).

2 O **2nd:** IPA published guidelines presenting examples of internal fraud and summarizing measures to combat it.
IPA "Guidelines for Preventing Insider Threats at Organizations Published" (http://www.ipa.go.jp/security/fy24/reports/insider/index.html) (in Japanese).

3 O **4th:** The Ministry of Internal Affairs and Communications published its Reinforcement Strategy on Smartphone Safety and Security, which summarized recommendations regarding the new issues associated with smartphones.
"Announcement of Reinforcement Strategy on Smartphone Safety and Security" (http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/130904_01.html).

4

5 S **5th:** In the lower house of the diet, a server outage prevented the electronic mail used in the Diet Members' Building from being read.

6 S **6th:** A paid news site for local authorities was accessed without authorization, and the website was altered to embed malicious code that exposed visitors to malware.

7 O **6th:** It was observed that the number of users of Tor had increased by several million from late August. It was estimated that this increase was caused by botnet use.
"How to handle millions of new Tor clients" (https://blog.torproject.org/blog/how-to-handle-millions-new-tor-clients).

8 O **6th:** A number of media outlets reported that the U.S. National Security Agency (NSA) had put backdoors in some of the encryption algorithms formulated by the National Institute of Standards and Technology (NIST), making decryption possible.
Subsequently, NIST released a statement denying the possibility that they had knowingly adopted vulnerable cryptographic standards ("Cryptographic Standards Statement" (http://www.nist.gov/director/cybersecuritystatement-091013.cfm)). In September they also announced they would recommended against the use of SP 800-90A (Dual_EC_DRBG) and perform a review. "SUPPLEMENTAL ITL BULLETIN FOR SEPTEMBER 2013 NIST OPENS DRAFT SPECIAL PUBLICATION 800-90A, RECOMMENDATION FOR RANDOM NUMBER GENERATION USING DETERMINISTIC RANDOM BIT GENERATORS, FOR REVIEW AND COMMENT" (http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf).

9

10

11 V **11th:** Microsoft published their Security Bulletin Summary for September 2013, and released four critical updates including MS13-067, MS13-068, and MS13-069, as well as nine important updates.
"Microsoft Security Bulletin Summary for September 2013" (http://technet.microsoft.com/en-us/security/bulletin/ms13-sep).

12 V **11th:** A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB13-21: Security updates available for Adobe Flash Player" (http://www.adobe.com/support/security/bulletins/apsb13-21.html).

13 V **11th:** A number of vulnerabilities in Adobe Reader and Acrobat that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB13-22 Security updates available for Adobe Reader and Acrobat" (http://www.adobe.com/support/security/bulletins/apsb13-22.html).

14 V **11th:** A number of vulnerabilities in Adobe Shockwave Player that could allow arbitrary code execution were discovered and fixed.
"APSB13-23: Security update available for Adobe Shockwave Player" (http://www.adobe.com/support/security/bulletins/apsb13-23.html).

15

16 O **12th:** As part of a project commemorating the 40th year of ASEAN-Japan friendship and cooperation, an ASEAN-Japan Ministerial Policy Meeting on Cyber Security Cooperation was held to discuss cooperation between countries in the field of cyber security at the ministerial level, and a Joint Ministerial Statement was adopted.
National Information Security Center (NISC), "ASEAN-Japan Ministerial Policy Meeting on Cyber Security Cooperation" (http://www.nisc.go.jp/press/pdf/aseanj_meeting20130911.pdf) (in Japanese).

17

18 V **18th:** Microsoft released an advisory due to the possibility of encrypted information on a server being disclosed through the exploitation of a vulnerability in ASP.NET. A limited attack using this vulnerability was confirmed on September 21.
"Microsoft Security Advisory (2416728) Vulnerability in ASP.NET Could Allow Information Disclosure" (http://technet.microsoft.com/en-us/security/advisory/2416728).

19

20 V **18th:** Microsoft released an advisory due to a vulnerability in Internet Explorer that could allow remote code execution when specially crafted websites were viewed using it.
"Microsoft Security Advisory (2887505) Vulnerability in Internet Explorer Could Allow Remote Code Execution" (http://technet.microsoft.com/en-us/security/advisory/2887505). This issue was fixed with "Microsoft Security Bulletin MS13-080 - Critical: Cumulative Security Update for Internet Explorer (2879017)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-080) on October 9.

21

22 S **18th:** For historical reasons there were alterations and DDoS attacks on a number of Web servers around this day. However, attacks were smaller in scale compared with those last year.

23 V **21st:** A vulnerability (CVE-2013-4316) in Apache Struts that could cause issues such as processes being carried out without a user's intention due to the Dynamic Method Invocation being enabled by default was discovered and fixed.
Apache Software Foundation, "Apache Struts 2 Documentation S2-019" (http://struts.apache.org/release/2.3.x/docs/s2-019.html).

24

25 O **22nd:** U.S. security company FireEye reported it had confirmed attacks targeting Japanese organizations through the exploit of an unpatched vulnerability in Internet Explorer.
See the following FireEye Blog post for more information. "Operation DeputyDog: Zero-Day (CVE-2013-3893) Attack Against Japanese Targets" (http://www.fireeye.com/blog/technical/cyber-exploits/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html).

26 O **25th:** The Ministry of Internal Affairs and Communications announced it would carry out a practical Cyber Defense Exercise using a large-scale simulated environment to improve cyber attack response capabilities.
"Implementation CYber Defense Exercise with Recurrence (CYDER)" (http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/130925_02.html).

27

28 S **26th:** Kaspersky Lab published a report on the "Icefog" APT campaign that targeted Japan and South Korea.
See the following Kaspersky Lab report for more information. "Kaspersky Lab exposes 'Icefog': a new cyber-espionage campaign focusing on supply chain attacks" (http://www.kaspersky.com/about/news/virus/2013/kaspersky_lab_exposes_icefog_a_new_cyber-espionage_campaign_focusing_on_supply_chain_attacks).

29

30 O **26th:** The 11th Assembly of the government's Council for Promotion of Information Security Measures (Liaison Conference for CISO, etc.) was held, and guidelines for implementing protective measures for work systems at each ministry were decided upon to protect important information from advanced cyber attacks such as targeted attacks.
National Information Security Center, "13th Assembly (September 26, 2013)" (http://www.nisc.go.jp/conference/suishin/index.html#2013_5) (in Japanese).

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

*Dates are in Japan Standard Time

■ Smartphone Threats

During the current survey period, smartphone vulnerabilities and related trends received widespread attention.

Researchers announced that some Motorola devices were collecting personal information without the users' intention. It was reported that the information collected included users' IDs and passwords for services such as external SNS, and that login warnings were sent from external services in what are thought to be attempts to log in using collected data.

At Black Hat USA 2013 held in the United States, it was reported that there was a vulnerability in Android OS that could allow files to be altered without breaking their signature in the case of legitimately signed apk files, etc. This was due to a vulnerability in the authentication process for the encrypted authentication of files. Additionally, another researcher announced that attacks on devices were possible using SMS due to issues with the encryption strength of the DES-based cryptographic communications used with some SIM cards. This SIM card vulnerability made waves in the press, etc., because many devices in Japan could potentially be targeted.

With the widespread use of mobile devices such as smartphones, these issues affect hundreds of millions of devices. The vulnerabilities and other issues presented here had limited impact, due in part to how swiftly fixes were made, or because they depended on specific conditions. However, because a single issue affects a large number of devices, and could turn into a major threat, we must continue to exercise caution.

■ Other

In August, the National Police Agency published "The State of Cyber Attacks in the First Half of 2013," which summarized the state of cyber attacks in the first half of fiscal 2013*18 This report indicated that "seed-sowing" attacks in which emails are sent to related parties purportedly to supply information, etc., as part of a targeted email attack had decreased. On the other hand, "interactive" attacks in which targeted emails are sent after exchanging emails containing work-related details with the attack target were on the rise. Many of the email exchanges apparently involved questions regarding recruitment or inquiries about product-related issues.

In July, the Telecom-ISAC Japan industry group for major telecommunications carriers and ISPs in Japan issued an alert recommending measures such as the application of patches and confirmation of settings due to vulnerabilities in certain products that related to a number of unauthorized login incidents*19. This organization has been conducting a survey aiming to assess the state of member ISP IP address ranges with regard to vulnerabilities in devices connected to networks in Japan since June*20.

In September, IPA published its "Guidelines for Preventing Insider Threats at Organizations," which presents examples of internal fraud, and facilitates the preparation of measures by providing a checklist for assessing the status of internal fraud countermeasures, and a Q&A section offering advice on countermeasures. This document explains the relevant measures, and covers the topics of early detection and preventing escalation, in a form that is easy for companies that had not considered internal fraud countermeasures to use.

IPA also published its "System Design Guide to Protect Against 'Targeted Email Attacks'," which covered new types of cyber attack, of which targeted email attacks are most prominent. It gave an overall picture of the intentions and background behind targeted attacks by analyzing them in detail, and summarized design techniques for system building, as well as measures to be taken by operators, for information systems at organizations as a whole. This guide analyzes different levels of targeted email attack, and indicates the countermeasures for each. It also presents a variety of initiatives for restricting activity and preventing spread as well as the theft of information when an organization is compromised, by implementing information system design and operational measures.

*18 National Police Agency, "The State of Cyber Attacks in the First Half of 2013" (http://www.npa.go.jp/keibi/biki3/250822kouhou.pdf) (in Japanese).
*19 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).
*20 Telecom-ISAC Japan, "A Survey on the Presence of Vulnerabilities in Network Devices" (https://www.telecom-isac.jp/news/news20130617.html) (in Japanese).

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 3 shows the circumstances of DDoS attacks handled by the IIJ DDoS Protection Service between July 1 and September 30, 2013.

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

There are many methods that can be used to carry out a DDoS attack, and the capacity of the environment attacked (bandwidth and server performance) will largely determine the degree of impact. Figure 3 categorizes DDoS attacks into three types: attacks on bandwidth capacity*21, attacks on servers*22, 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 628 DDoS attacks. This averages to 6.9 attacks per day, indicating an increase in the average daily number of attacks compared to our prior report. Server attacks accounted for 75.3% of all incidents, while compound attacks accounted for 22.6%, and bandwidth capacity attacks 2.1%.

The largest attack observed during the period under study was classified as a compound attack, and resulted in 3.2 Gbps of bandwidth using up to 322,000 pps packets.

Of all attacks, 71.3% ended within 30 minutes of commencement, 28.5% lasted between 30 minutes and 24 hours, and 0.2% lasted over 24 hours. The longest sustained attack for this period was a compound attack that lasted for one day, eight hours, and 27 minutes (32 hours and 27 minutes).

Each year during this period, many DDoS attacks are observed around historic dates. We confirmed that the number of DDoS attacks was once again higher than normal this year between September 15 and September 18. Regarding the scale of attacks, a compound attack that peaked at 2.5 Gbps and around 700,000 pps was observed.

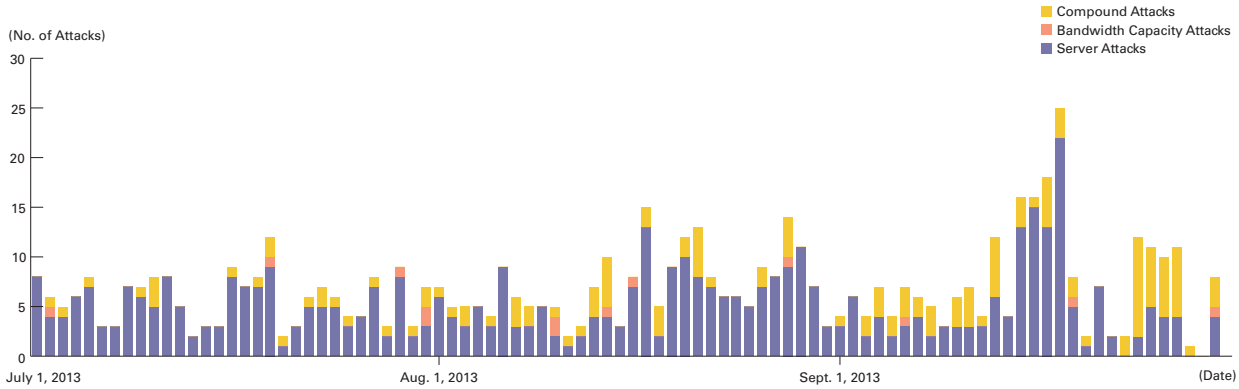


Figure 3: Trends in DDoS Attacks

*21 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.

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

In most cases, we observed an extremely large number of IP addresses, whether domestic or foreign. We believe this is accounted for by the use of IP spoofing*23 and botnet*24 usage as the method for conducting DDoS attacks.

Backscatter Observations

Next we present our observations of DDoS attack backscatter using the honeypots*25 set up by the MITF, a malware activity observation project operated by IIJ*26. By monitoring backscatter it is possible to detect some of the DDoS attacks occurring on external networks as a third party without any interposition.

For the backscatter observed between July 1 and September 30, 2013, Figure 4 shows the sender's IP addresses classified by country, and Figure 5 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 49.6% of the total during the target period. Attacks were also observed on 22/TCP used by SSH, 30800/TCP thought to be related to games, and 1935/TCP used for streaming communications, as well as on ports not normally used such as 25565/TCP.

Looking at the origin of backscatter thought to indicate IP addresses targeted by DDoS by country in Figure 4, for the current survey period the United States accounted for the largest ratio at 21.6%. France and the Netherlands followed at 13.8% and 8.7%, respectively.

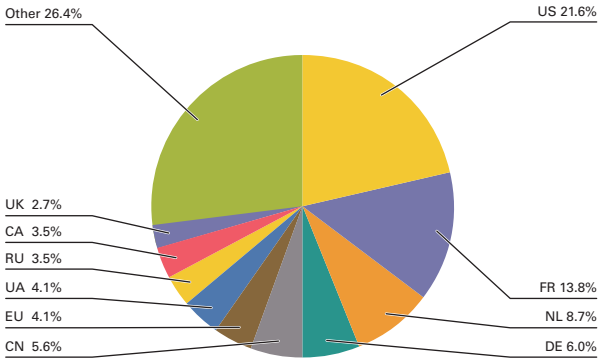


Figure 4: Distribution of DDoS Attack Targets According to Backscatter Observations (by Country, Entire Period under Study)

Regarding particularly large numbers of backscatter packets observed by targeted port, there were attacks on the Web servers (80/TCP) for a hosting provider in the Philippines on August 27. Between August 13 and 14, attacks were observed on the Web servers of a hosting provider in Lebanon. Attacks on Web servers for a hosting provider in China were observed on September 18.

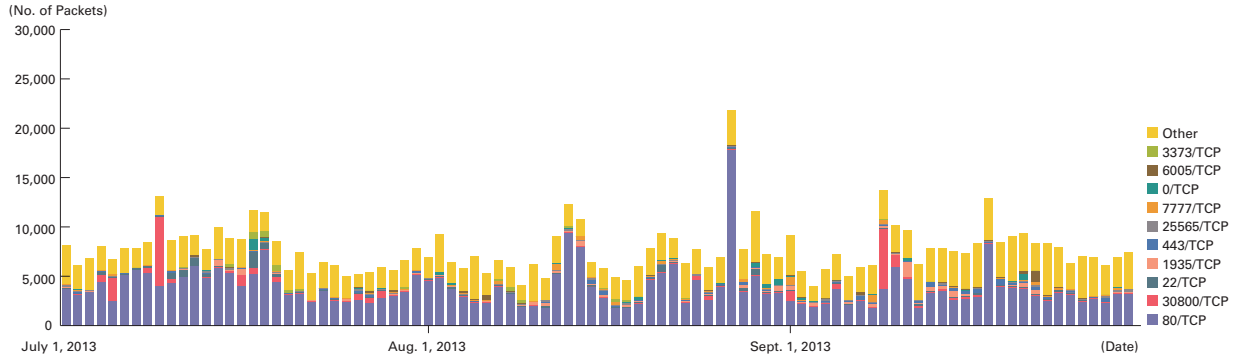


Figure 5: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)

*23 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.

*24 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.

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

*26 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 September 11, attacks on 1935/TCP targeting a number of servers for multiple hosting providers in Sweden and Canada were observed. On July 9 and September 9 there were attacks on 30800/TCP targeting the servers of a number of hosting providers in France and the Netherlands. 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 in September on sites related to North Korea thought to have been carried out by Anonymous.

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the MITF*27, a malware activity observation project operated by IIJ. The MITF uses honeypots*28 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 6 shows the distribution of sender's IP addresses by country for communications coming into the honeypots between July 1 and September 30, 2013. Figure 7 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, 23/TCP used for telnet, ICMP echo requests, and 53/UDP used for DNS.

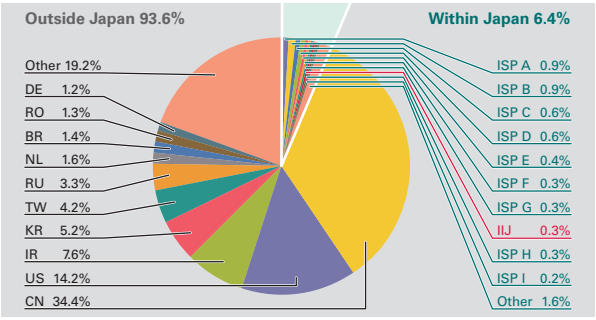


Figure 6: Sender Distribution (by Country, Entire Period under Study)

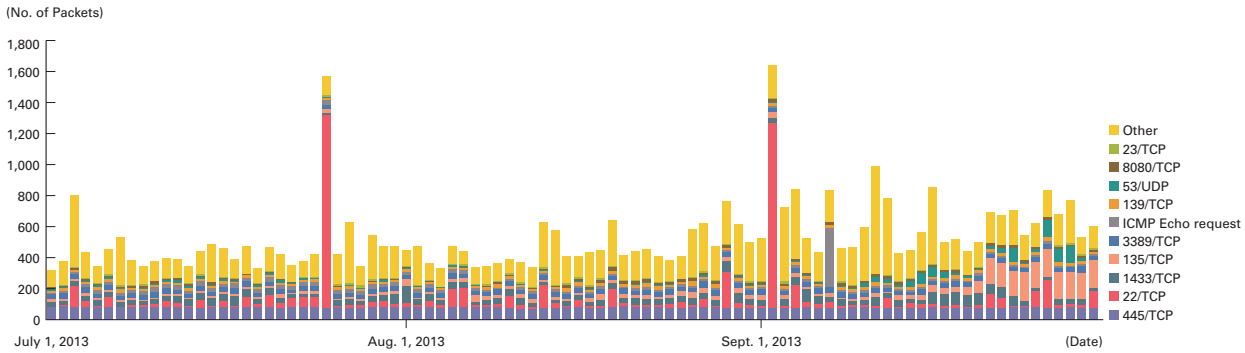


Figure 7: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

*27 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.

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

Communications thought to be SSH dictionary attacks also occurred during the current survey period. For example, concentrated communications were observed coming from IP addresses allocated to China on July 24, and South Korea on September 2. After mid-September, concentrated 53/UDP communications from IP addresses allocated to China increased to a level dozens of times higher than usual. After looking into the matter, we believe this was scanning behavior looking for open resolvers for carrying out DNS amplification attacks. Furthermore, between late August and mid-September, access from IP addresses allocated to China increased to around double normal levels. This is thought to be scanning behavior aimed at finding alterable SQL servers. In both cases, communications targeted an extremely wide range of IP addresses, implying that they were searching for servers that could be attacked, or that could be used in attacks. 135/TCP communications from IP addresses allocated to the United States also suddenly increased to several dozen times previous levels at the end of September. Looking into the details of these communications, ServerAlive2 requests were being delivered using DCOM IOXIDResolver operations. Because this is a mechanism for confirming whether a Microsoft RPC server is operating on a remote host, we believe it was scanning behavior for RPC servers. Additionally, although communications arrived from over 100 unique IP addresses allocated to the United States during the period of rapid increase, two AS numbers accounted for 80% of total traffic volume. This deviation in the attacker's infrastructure is one of the characteristics.

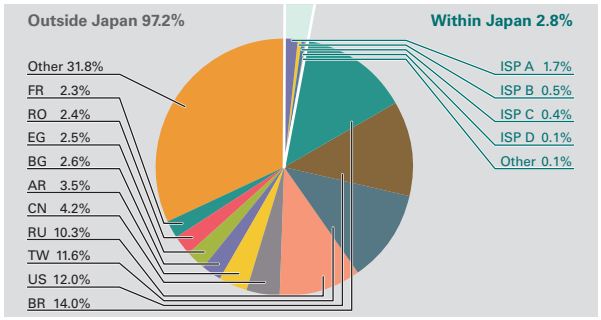


Figure 8: Distribution of Acquired Specimens by Source (by Country, Entire Period under Study, Excluding Conficker)

Malware Network Activity

Figure 8 shows the distribution of the specimen acquisition source for malware during the period under study, while Figure 9 shows trends in the total number of malware specimens acquired. Figure 10 shows trends in the number of unique specimens. In Figure 9 and Figure 10, the trends

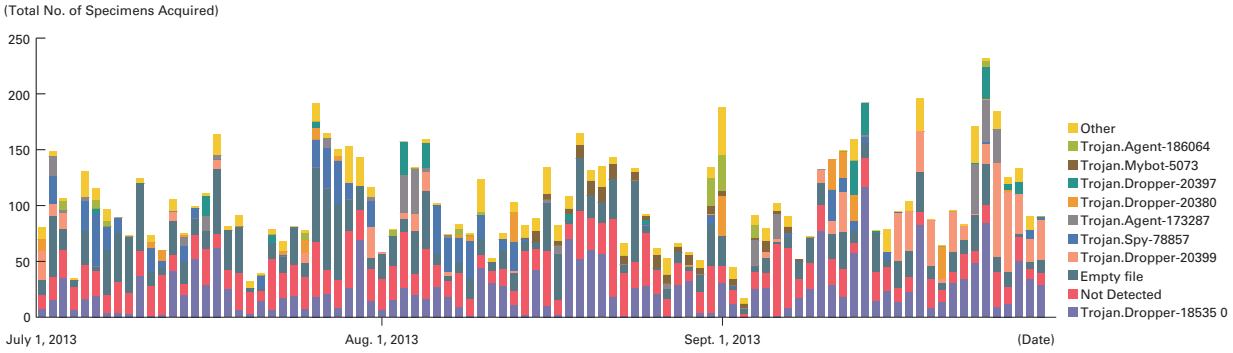


Figure 9: Trends in the Total Number of Malware Specimens Acquired (Excluding Conficker)

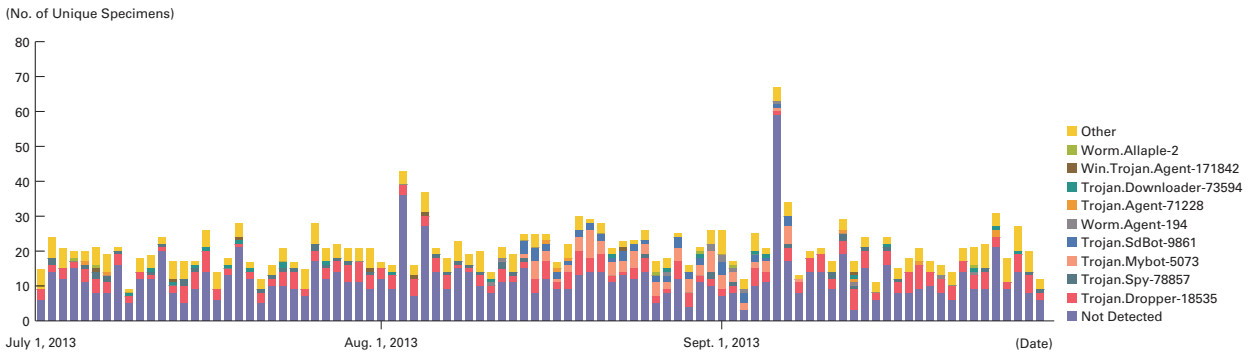


Figure 10: Trends in the Number of Unique Specimens (Excluding Conficker)

in the number of acquired specimens show the total number of specimens acquired per day*29, while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*30.

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 9 and Figure 10 we have detected Conficker using multiple anti-virus software packages, and removed any Conficker results when totaling data.

On average, 105 specimens were acquired per day during the period under study, representing 21 different malware. After investigating undetected specimens more closely, worms*31 from IP addresses allocated to the United States and France were also observed continually between July and early August, and a type of bot*32 controlled by a Philippines IRC server was observed on a constant basis in mid-August.

Under the MITF's independent analysis, during the current period under observation 79.4% of malware specimens acquired were worms, 15.3% were bots, and 4.9% were downloaders. In addition, the MITF confirmed the presence of 21 botnet C&C servers*33 and 10 malware distribution sites.

■ Conficker Activity

Including Conficker, an average of 34,387 specimens were acquired per day during the period covered by this report, representing 788 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 5% compared to the previous survey period. Unique specimens were also down by about 3%. According to the observations of the Conficker Working Group*34, as of October 4, 2013 (note: because the Conficker Working Group's data between September 30 and October 3 was extremely scarce, it was treated as anomalous, and figures for this day were used instead), a total of 1,450,964 unique IP addresses are infected. This is a drop of approximately 45% compared to the 3.2 million PCs observed in November 2011, but it demonstrates that infections are still widespread.

*29 This indicates the malware acquired by honeypots.

*30 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.

*31 WORM_DEBORM. AP (http://about-threats.trendmicro.com/Malware.aspx?id=36201&name=WORM_DEBORM.AP&language=au).

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

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

*34 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*35. 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 11 shows the distribution of SQL injection attacks against Web servers detected between July 1 and September 30, 2013. Figure 12 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 54.1% of attacks observed, while the United States and Morocco accounted for 15.2% and 9.8%, respectively, with other countries following in order.

There was little change from the previous period in the number of SQL injection attacks against Web servers that occurred. Attacks from Morocco 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 specific attack sources in Japan directed at specific targets between September 9 and 11. On July 30, attacks from specific attack sources in Morocco directed at a specific target also took place. On August 14, there were attacks from specific attack sources in the United States on specific targets, as well as attacks from specific sources in the United States, Germany, and Great Britain on other specific targets. 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.

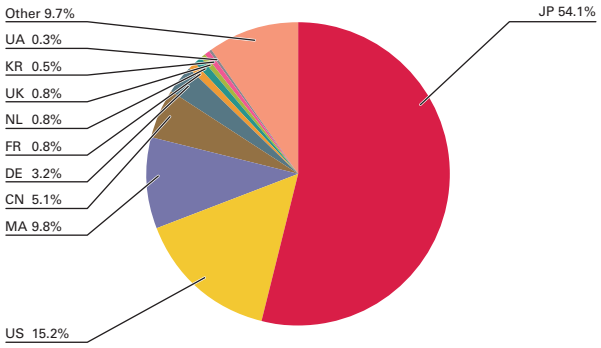


Figure 11: Distribution of SQL Injection Attacks by Source

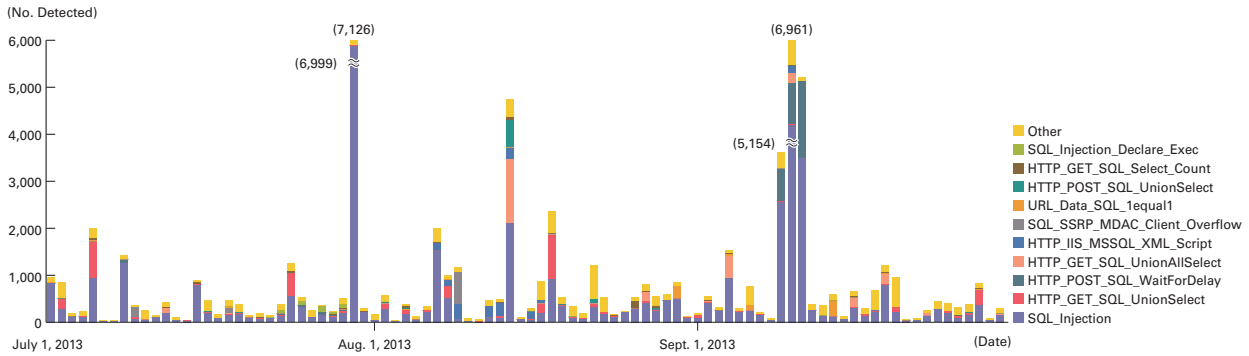


Figure 12: Trends in SQL Injection Attacks (by Day, by Attack Type)

*35 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, and discuss the PlugX RAT used in targeted attacks, a series of targeted email attacks, and the Bitcoin virtual currency.

1.4.1 The PlugX RAT Used in Targeted Attacks

PlugX is a type of RAT*36 also known as Korplug and Gulpix that is frequently used in targeted attacks, along with Poison Ivy and others. IIJ obtained specimens that were actually used in recent targeted attacks, and analyzed them in detail. Here we report on the functions of these specimens, and consider techniques for detecting this malware.

■ An Overview of PlugX

PlugX was discovered in March 2012, and since its discovery it has been updated continually. This malware includes basic RAT functions such as file operations (creation and copying, downloading and uploading, execution and stopping, etc.), registry operations, starting and stopping of services, logging of keyboard input, screen capture, and remote shell execution, as well as port scanning and functions for connecting to SQL servers and stealing information. As indicated by its name, the fact it can be expanded using plug-ins is another characteristic.

■ Characteristics

Figure 13 shows the execution flow when the specimens obtained by IIJ were executed. A ZIP file email attachment is sent, which contains an EXE file when unzipped. If an email recipient double-clicks this file, the dropper is executed. This dropper creates a code-signed EXE (a legitimate application, not malware) and a DLL for loading PlugX (PlugX loader) in the same folder. It then executes the code-signed EXE. When the EXE is executed, its dependent DLL is loaded, but because the PlugX

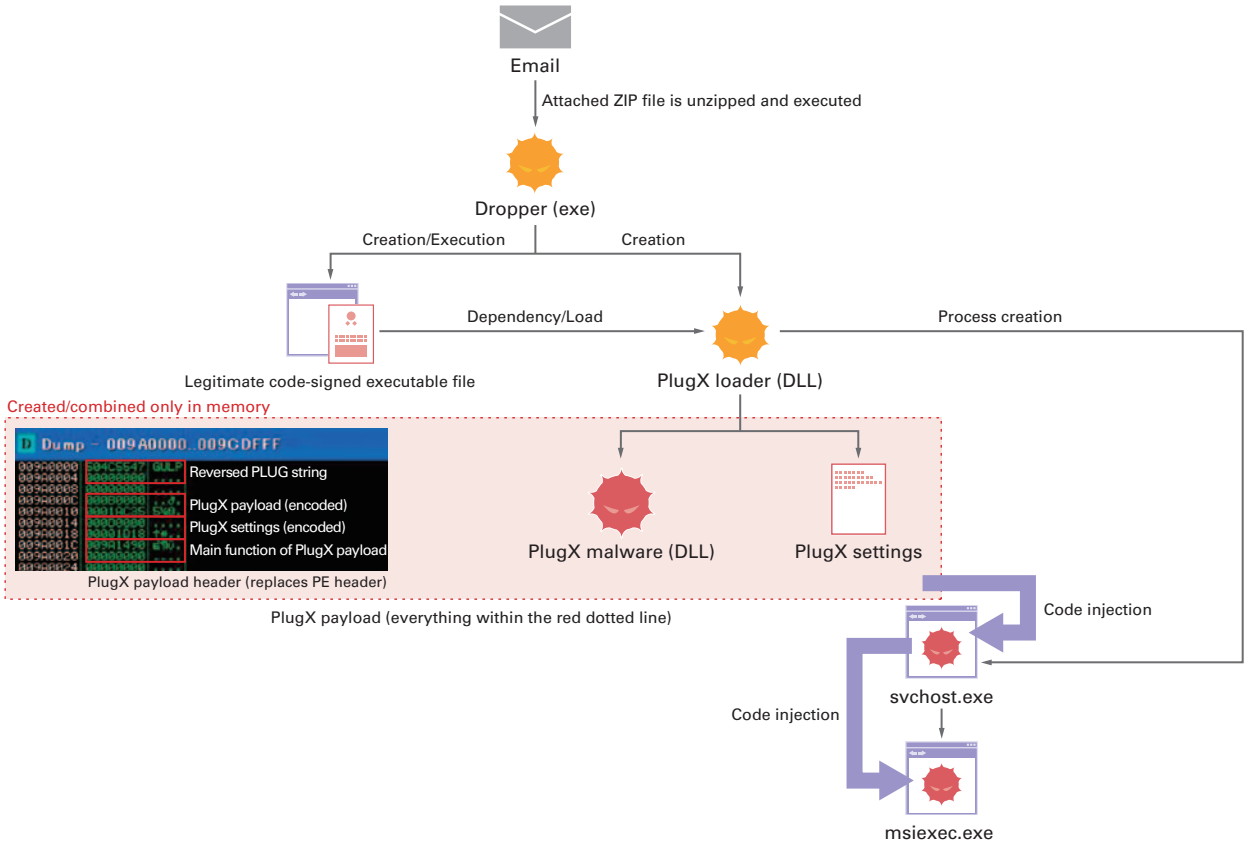
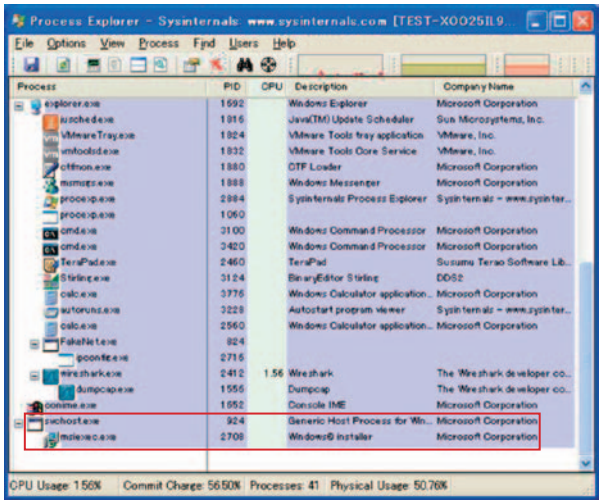


Figure 13: PlugX Execution Flow

*36 An abbreviation of Remote Administration Tool, which is software for remotely controlling a host in which it is installed. It is also sometimes called a Remote Access Tool or Remote Access Trojan.

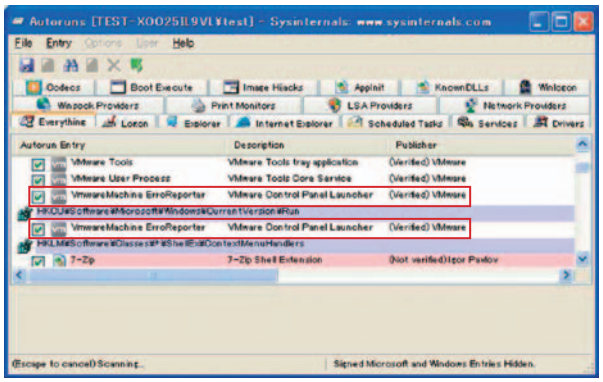
loader has the same name as the dependent DLL, the DLL loading priority is misused (a DLL in the same folder is given higher loading priority) to load the PlugX loader instead of the legitimate DLL, executing the code. The PlugX loader decodes the PlugX malware and DLL in memory, and begins executing the PlugX malware by injecting its code into a svchost.exe process that the PlugX loader created itself. However, there are also standalone specimens that do not inject code into svchost.exe or exploit the DLL loading priority. Instead, they conduct the PlugX loader processing with a single executable file (an unsigned EXE file), into which the PlugX malware and its settings are deployed. When carrying out code injection, the PE header is changed to a header beginning with "GULP" (PLUG backwards). This header stores address pointers and size information for the encoded settings and its own code, as well as a pointer to the main function of PlugX. Areas other than the PE header for the PlugX malware (code and data) are stored after the header. These injected pieces are collectively known as the PlugX payload. The injected PlugX payload creates an msiexec.exe process, and injects code into that also. Meanwhile, because the PlugX loader process itself terminates, when checking with a tool such as Process Explorer*37, only svchost.exe and msiexec.exe will appear to be running (Figure 14).

The PlugX loader also adds registry entries to execute the file automatically when a computer is booted up, but as mentioned previously, the registered executables are code-signed EXE files. For this reason, when searching for traces of malware using tools such as Autoruns*38, it appears as if correctly code-signed programs are registered, making the malware hard to detect*39 (Figure 15).



The red box indicates processes created by PlugX, but because both are legitimate Windows executables, it is difficult to detect them as malware at a glance.

Figure 14: Appearance When Viewed in Process Explorer



The two red boxes indicate registry entries added by PlugX, but because they are correctly code-signed executable files, Autoruns has not flagged them in red or yellow for review.

Figure 15: Registry Entries

*37 Process Explorer is a tool for viewing the status of running programs that is distributed with Microsoft's Windows Sysinternals (http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx). It provides access to more detailed information than the standard Windows Task Manager.

*38 Autoruns is a tool for displaying a list of programs that are executed automatically when Windows starts. Like Process Explorer, it is distributed with Microsoft's Windows Sysinternals (http://technet.microsoft.com/en-us/sysinternals/bb963902). Because analysis can also be performed offline, it is a useful tool for responding to incidents.

*39 In addition to the technique of misusing the DLL loading priority like PlugX, other mechanisms have been used to evade detection by Autoruns. In some cases, a code-signed EXE or DLL with a buffer overflow vulnerability is prepared and registered, and this vulnerability is then exploited by passing on a long data string including shellcode or the malware itself as the parameter when executing the file. This causes a buffer overflow that executes arbitrary code, and as a result executes the malware. For example, at VB2013 in October 2013, there were reports that malware known as Simbot attempted to evade detection by exploiting this trick (http://www.virusbtn.com/pdf/conference_slides/2013/Szappanos-VB2013.pdf) Therefore, it is also necessary to keep this in mind and check for it when responding to incidents.

TCP, UDP, ICMP, and HTTP can be used for communications with C&C servers, and it is also possible to use a combination of multiple communication methods for an IP address. Because communications are encoded with a unique algorithm, it will be difficult to identify PlugX communications until this is decrypted. However, there are a number of characteristics (the POST request and path portion is "/update?id=8-digital hexadecimal number," and unique HTTP headers such as "X-Session" as used) when carrying out HTTP communications, as indicated in Figure 16. Additionally, the architecture allows proxy servers to be used for TCP and HTTP communications. Four C&C servers can be statically defined in the settings, which also include URLs to download HTTP C&C server settings.

Another characteristic is the function for bypassing UAC (User Account Control). UAC was introduced in Windows Vista, but from Windows 7 onward it has been set to one level below the maximum by default. At this level, UAC pop-ups only appear when changes are made to programs. Actions thought to have been carried out directly by users do not cause the UAC pop-up to appear, and are automatically elevated to administrator privileges. PlugX takes advantage of this to bypass UAC and gain administrative privileges without the user being aware by misrepresenting actions as being carried out by the user.

■ Detection Method

PlugX demonstrates the previously-mentioned characteristics when conducting HTTP communications. Because they are hardcoded into PlugX itself, and modifying them would require modification of the C&C servers that PlugX communicates with, they are comparatively difficult characteristics to change*40. Gateways and IPS systems can detect infected PCs by checking for these characteristics. However, in a specimen recently obtained by IIJ, the unique HTTP headers had each been changed from "MJ1X" to "MJ4X"*41. Consequently, when detection using HTTP header characteristics is not possible, it would be a good idea to also look for the following characteristics in the host's memory.

When PlugX malware injects code into svchost.exe, as mentioned before the header is changed to one starting with "GULP". Although the process targeted for injection can be changed in the settings, the "GULP" string is not only found at the start of the header, but is also hardcoded as a string in the code for confirming that PlugX has been executed in the injection target, so this string would be one of those hard for anyone but the developer to change. Furthermore, this string is found at the beginning of the memory space in unencrypted form, making it easy to detect. The allocated memory space for PlugX also contains the PAGE_EXECUTE_READWRITE attribute. This means you should be able to detect it by scanning the memory space for all processes, and checking spaces beginning with this string, as well as their attributes. You can check for the following in combination with these characteristics to reduce the number of false positives.

Figure 16: HTTP Communications with C&C Servers

*40 In recent years, malware has been traded in underground forums as a commercial product, and a business model has been established. Examples of this kind of model include exploit kits such as the Blackhole exploit kit, and crimeware kits such as ZeuS (including variants like Citadel and Gameover) and SpyEye that have been involved in a sudden surge of incidents in Japan. PlugX also has a demo version, so this model may have been adopted in its case as well. The existence of a demo version of PlugX has been reported at the following site (http://www.lastline.com/an-analysis-of-plugx). This demonstrates that division of labor is more and more common these days, and developers and users (attackers) are often not the same people. For this reason, users can only change the configuration for limited parts of the malware, such as the C&C server name or the path part of the URL, settings for enabling or disabling a number of settings, or the key or value for registration to the registry. It is relatively difficult to freely change the code in the way that developers with the source code can. Additionally, there are parts that are comparatively difficult to change even for developers. For example, to change the communication protocol, etc., the C&C server code must also be changed at the same time, leading to compatibility issues with malware that is already communicating. As a result, we define elements such as the communication protocol, the encoding/decoding algorithm for communications or data, the values that malware use to identify its code, and the Windows API necessary to implement the malware's functions, as comparatively difficult characteristics to change.

*41 IIJ has obtained and analyzed several dozen types of PlugX specimen, but only a very small number of these that were obtained recently had a different unique HTTP header. All specimens up to that point had the characteristics shown in Figure 16. Consequently, although it is not clear whether this type of modified specimen will become prevalent, or if they are just rare cases, it is necessary to at least consider the fact that changes may have been made.

- **PlugX Encoding/Decoding Routine Characteristics**
  PlugX has a function for encoding communications and configuration data. This algorithm uses a distinctive immediate value, such as 0x11111111, 0x22222222, 0x33333333, or 0x44444444.

- **String Related to Privileged Operations**
  Debug privileges such as "SeDebugPrivilege" are not usually requested by standard applications.

Memory can be checked using Mandiant's Redline*42 or Volatility Framework*43.

■ Countermeasures

To avoid being infected with this kind of malware, it is necessary to implement a several layers of defense, including conventional measures such as keeping your OS and all installed applications up to date, as well as using anti-virus software, and of course keeping it updated to the latest version.

For example, by restricting the areas where executables can be run using the Software Restriction Policy included as standard in Windows OSes after Windows XP, or alternatively AppLocker, it is possible to prevent the execution of executable files in "Desktop", "My Documents", or "Temp" folders. This prevents executables disguised as document files from being run when they are opened by mistake, and stops malware located into the temp folder from being executed when vulnerabilities have been used. Because most of the specimens obtained by IIJ are also placed under the user directory, it is possible to prevent infection by restricting executable areas to the "C:\Program Files" and "C:\Windows" directories. Additionally, because DLLs and other libraries are not restricted by default, placing restrictions on them can prevent DLLs under the user directory from being loaded, as they are in the case of this malware. As mentioned previously, PlugX has a function for bypassing UAC, but changing UAC to the highest level on Windows 7 or later OSes prevents UAC from being circumvented. In the event you are infected, it also enables you to restrict or delay the attacker's subsequent actions using PlugX. Additionally, because there are many cases of malware being installed via malicious document files, you can use EMET*44 to establish mitigation measures for unknown vulnerabilities. This mitigates exploits targeting vulnerabilities and the subsequent execution of malware. Enabling the Click-to-Play function*45 implemented in Mozilla Firefox and Google Chrome also prevents attacks on browser plug-ins when accessing the Web, protecting you from them.

It is also necessary to gather information on incidents, and consider and implement a system that can detect issues at all times. The IOC which were discussed as methods for detecting the incidents covered here are published on a number of websites by volunteers, but most of them can easily be changed in the settings by attackers, such as the file names, hash values, and registry keys. For this reason, although they can be applied to past incidents, it is likely that they will not be detectable in incidents that occur in the future. Consequently, by analyzing malware in detail, and creating IOC rules based on the previously-mentioned characteristics that are difficult for attackers to change, it will be possible to detect malware on an ongoing basis for long periods of time. At this time, because characteristics are hidden due to obfuscation or being packaged when investigating files, conducting a close inspection of the code and data currently being executed in memory will make more effective detection possible.

1.4.2 A Series of Targeted Email Attacks

Between late August and late October 2013, repeated attacks were made on a certain organization by sending emails with RAT attached. Here we discuss this series of attacks, as well as the response made by the organization that was targeted.

*42 Mandiant Redline (http://www.mandiant.com/resources/download/redline) is an incident response tool for tracking down traces of malware and other threats in disk and memory images. In addition to the predefined rules, it is also possible to define your own rules in XML format, which are called IOC (Indicators of Compromise).

*43 Volatility Framework (https://www.volatilesystems.com/default/volatility) is a tool for analyzing memory images. It also has a module that uses YARA (http://code.google.com/p/yara-project/) for conducting pattern matching, which is useful when responding to incidents.

*44 EMET (Enhanced Mitigation Experience Toolkit) is a tool provided by Microsoft for mitigating the exploitation of software vulnerabilities.

*45 Click-to-Play is a function that prompts for user confirmation (via a click) instead of executing plug-ins automatically. Because the plug-in display area is often concealed for drive-by download attacks, users will never click it accidentally.

■ An Overview of the Series of Emails

The first email was sent on August 29, and contained the text shown in Figure 17. This email has a ZIP file attached with a name hinting at the "contact list" mentioned in the body text, and this had an executable file (EXE) of the same name archived within it. The executable file is the RAT software, but the icon image makes it appear to be a Microsoft Excel document file. This means the RAT will be executed if the recipient is fooled by the icon into double-clicking the file without checking the extension. The attached RAT was Poison Ivy, and the C&C server, account ID, and password were configured as shown in Figure 18. We believe that the fact part of the corresponding organization's domain name was used in the account ID clearly indicates that this email was not an indiscriminate attack, but targeted the organization in question.

Starting with this email, a total of 11 types of targeted email were sent to the corresponding organization up to October 21.

■ Common Characteristics

Table 1 shows a list of the targeted emails sent to this organization. Most of the 11 types of email sent had characteristics A to F below in common.

A. Poison Ivy or PlugX attached (11/11)
B. A frequently used string[*46] was set as the C&C server password for Poison Ivy (7/7)
C. A free webmail service was used to send the email (11/11)
D. An IP address from a specific ISP in Japan was used to connect to the webmail service (9/10)
E. The text and attachment name were disguised to appear as work-related correspondence within the corporate organization (10/11)
F. The RAT executable file had a misleading icon and was stored in a ZIP archive (10/11)

The series of targeted emails were divided with regard to the type of RAT attached (Poison Ivy or PlugX), but both types had characteristics C to F in common. It is thought highly likely that the group with Poison Ivy attached were sent by the same entity, due to the points in common such as the C&C server and password used.

The PlugX malware used in email (4) had parts that appeared different to the PlugX malware used in emails (9) to (11), such as the C&C server and the sender's IP address. However, analysis results for the attached PlugX files demonstrated that the same details were set for the installation information and service names.

To: 個人、ML 等
From: *部署名__個人名* <*個人名*@aol.com>
Subject: Fw:_08/29(木)_職員連絡網の最新版データ送付
Date: Thu, 29 Aug 2013 04:10:26 -0400 (EDT)

各位

お世話になります。

標記の件、添付データを送付いたしますのでよろしくご査収ください。

「旧名簿」とありますが電話番号と住所、E-MAILは最新データです。

個人名
****
組織名
部署名 個人名
組織の住所
組織のレンジに近い電話番号
組織のレンジに近いFAX番号
E-mail: *個人名*@*組織のドメイン*

組織名(英文)
WEB: *組織のWebサイトURL*
****

Figure 17: Targeted Email (1) Sent on Thursday, August 29

Additionally, the PlugX malware used in emails (9) to (11) was set to the same C&C server as the Poison Ivy malware used in email (8), suggesting that the entire series of attacks was carried out by the same entity.

Although all emails had characteristic C in common, the use of a legitimate email service is thought to be for the purpose of bypassing SPF and DKIM, which detect fraudulent email, rather than to make the emails appear to be from a personal email address.

C&C server: drives.methoder.com (50.2.160.125)
Account ID: drive.●829
Password: keaidestone

*The "●" is part of the corresponding organization's domain name

Figure 18: Configuration Details of the Poison Ivy Malware Attached to Email (1)

*46 FireEye's "Poison Ivy: Assessing Damage and Extracting Intelligence" (http://www.fireeye.com/resources/pdfs/fireeye-poison-ivy-report.pdf) reports that "keaidestone" and "smallfish" are both strings used as C&C server passwords.

Meanwhile, focusing on the quality of the attacks, deficiencies such as the following stand out.

a. Japanese text is used, but in places the wording and formatting is unnatural.
b. The text contained details such as division names commonly found at corporate organizations, as well as common Japanese surnames, but in some cases these did not exist at the organization.
c. Known and relatively prominent RATs were employed, and the same C&C server was used repeatedly.

Although the attacks continued for approximately two months, no substantial changes were seen. Details such as the C&C server account name settings for the Poison Ivy malware in emails (5) and (6) give the impression of being created in assembly-line fashion.

Considering the previously mentioned common points, and these quality-related circumstances, we believe these were not advanced attacks planned especially for the organization that was targeted. Instead, while targeting individual organizations such as the one we examined here, they may have been part of semiautomated, proceduralized, unsophisticated attacks made on a comparatively wide range of targets. IIJ has actually confirmed attacks made on at least seven other organizations that used C&C servers with addresses identical to or neighboring those for the RATs used in the attacks discussed here.

■ Response at the Targeted Organization and Impact

Of the series of emails, email (2) was detected and deleted by the anti-virus software for the mail gateway used at the organization. Emails (9) through (11) were deleted by an attachment filter set for the mail gateway. This attachment filter was set by the organization after email (8) was received. It blocks emails that have executable files attached.

Table 1: The Series of Targeted Emails

	Date & Time of Transmission (JST)	Sender	Subject	Character Encoding	Attachment Name	Infection Method	Cover Icon	Malware (RAT)	Sender Client (IP Address Used by Web Mailer)	C&C Server	PI ID	PI Password
(1)	17:10 on Thursday, August 29	▲@aol.com	F w:__8月29日(木)__職員連絡網の最新版データ送付	UTF-8	130829_連絡網(旧連絡網・使用不可.zip)	EXE (cover icon used)	XLS	Poison Ivy	126.114.231.116 (JP)	drives.methoder.com 50.2.160.125 (USA)	drive.●829	keaidestone
(2)	13:10 on Friday, August 30	▲@mail.goo.ne.jp	平成25年度後半年行政業務要点	UTF-8	平成25年度後半年行政業務要点.doc	CVE-2012-0158	--	Poison Ivy	(No corresponding header)	scrlk.exprenum.com 50.2.160.125 (USA)	GoodLuck830	keaidestone
(3)	15:30 on Thursday, September 5	▲@aol.com	平成25年度下期決算に向けての作業について	UTF-8	平成25年度下期決算に向けて.zip	EXE (cover icon used)	XLS	Poison Ivy	126.114.229.210 (JP)	daddy.gostudyantivirus.com 50.2.160.84 (USA)	●0905	smallfish
(4)	15:20 on Friday, September 13	▲@yahoo.co.jp	ゴーヤー収穫のお知らせ	GB2312 (executable file name only)	130924行政現場視察(防衛省).zip	EXE (cover icon used)	--	PlugX	155.69.203.4 (SG)	– 54.250.220.230 (AMAZON)	–	–
(5)	12:50 on Tuesday, September 17	▲@aol.com	【締切09-17】2013年駐在員執務体制確認依頼の件	UTF-8	20130917_執務体制確認依頼書.zip	EXE (cover icon used)	XLS	Poison Ivy	126.19.84.213 (JP)	daddy.gostudyantivirus.com 50.2.160.84 (USA)	XXXXXXXXXX	smallfish
(6)	12:50 on Tuesday, September 17	▲@aol.com	【報告】安全定期報告提出日のご案内	UTF-8	20130917 安全定期報告提出日のご案内.zip	EXE (cover icon used)	PDF	Poison Ivy	126.19.84.213 (JP)	daddy.gostudyantivirus.com 50.2.160.84 (USA)	ZZZZZZZZZ	smallfish
(7)	13:50 on Tuesday, September 24	▲@yahoo.co.jp	【新卒採用】履歴書を送付	UTF-8	▲.zip	EXE (cover icon used)	XLS	Poison Ivy	126.19.86.102 (JP)	saiyo.exprenum.com 54.248.202.112 (AMAZON)	saiyo0924	keaidestone
(8)	15:50 on Tuesday, September 24	▲@aol.com	【送付】職員連絡網の最新版データ送付	UTF-8	20130924_職員連絡網最新版.Zip	EXE (cover icon used)	DOC	Poison Ivy	126.65.195.56 (JP)	saiyo.exprenum.com 54.248.202.112 (AMAZON)	saiyo.ex	keaidestone
(9)	16:31 on Monday, October 21	▲@aol.com	【重要】(事前連絡)合同会議並びに定期大会調整状況について	UTF-8	合同会議並びに定期大会調整状況.zip	EXE (cover icon used)	XLS	PlugX	126.15.4.120 (JP)	saiyo.exprenum.com 54.248.202.112 (AMAZON)	–	–
(10)	16:32 on Monday, October 21	▲@aol.com	Fw:出版契約書	UTF-8	20131021 仕様書_▲.zip	EXE (cover icon used)	XLS	PlugX	126.15.4.120 (JP)	saiyo.exprenum.com 54.248.202.112 (AMAZON)	–	–
(11)	16:33 on Monday, October 21	▲@aol.com	Fw:自著紹介	UTF-8	20131021 (月)自著紹介.zip	EXE (cover icon used)	XLS	PlugX	126.15.4.120 (JP)	saiyo.exprenum.com 54.248.202.112 (AMAZON)	–	–

●: Part of the domain name of the organization targeted by the attack ▲: An arbitrary account name related to the sender's name that appears in the email text

To handle emails that were delivered to the end point without being blocked along the way, an organization-wide alert including the email text was issued each time the organization received a targeted email. However, it was not possible to completely prevent infection.

Because it is not possible to entirely avoid infections with this type of attack, it is important to provide a follow-up response under the assumption that infections will occur. At the organization in question, the following incident response flow was applied each time an email was delivered to the end point, as was the case with emails (1) and (3) through (8).

1. Employees who think an email is suspicious report it to the department in charge (= incident detection)
2. The attachment (RAT) is analyzed
3. Based on the analysis results, communications with the C&C server are blocked (firewall/DNS/proxy, etc.)
4. Examination of infected PCs (PCs are identified from the traffic logs, and an appropriate forensic investigation is carried out)

Each time an attack occurred, steps one through three were implemented comparatively quickly, so the organization did not suffer any ill effects from the series of attacks, such as information leaks or the destruction or sabotage of data.

■ Countermeasure Policy

Regarding emails from the series of targeted emails that could not be blocked using anti-virus software or mail server settings, the organization detected the incidents through the reports of employees who received the emails. However, depending on the number of users emails were delivered to, as well as how well they were disguised, incidents may have gone unreported. To be ready when a RAT infection occurs due to this kind of attack, it would be best to prepare a system of internal measures*47 for detecting and blocking suspicious communications and authentication attempts when computers in an organization are infected.

We also recommend the following measures be taken when you have already been the victim of targeted email attacks, under the assumption that attacks will continue to occur.

- Block the C&C servers used in past attacks, as well as neighboring IP addresses (firewall)
- Block domains associated with C&C servers used in past attacks (DNS, proxy, firewall)
- Block C&C communication patterns used in past attacks (proxy, IPS)
- Block attachments containing executable files (EXE, DLL, SCR, etc.)
- Reinforce internal network monitoring systems (record additional details in communication logs, and increase the frequency of analysis, etc.)

This will not protect against all targeted email attacks, but it should be somewhat effective against semiautomated, proceduralized targeted email attacks that are made on a comparatively wide range of targets, such as those discussed here.

1.4.3 The Bitcoin Virtual Currency

In this section we discuss Bitcoin, which has begun to take hold as a new form of currency among some Internet users. Bitcoin has a number of benefits compared to transactions using actual money. As a result, many transactions have been carried out using this currency since it was created in January 2009. Under this scheme, a proof-of-work system was implemented for the mining process that creates the currency, making it possible to convert computational resources into virtual value. Now it is also possible to exchange bitcoins for actual money, use them for payment at stores, and buy real-world products with them over the Internet, demonstrating that they are gradually becoming recognized as a true currency. Here, we explain the technology behind the Bitcoin virtual currency, and examine incidents and troubles that have occurred in relation to it.

Bitcoin is a virtual currency system that uses a P2P network and cryptographic technology to enable the circulation of coins while ensuring the anonymity of users. An article by an anonymous researcher or researchers going by the name

*47 See "The System Design Guide for Thwarting Targeted Email Attacks" (http://www.ipa.go.jp/security/english/newattack_en.html) for more information.

Satoshi Nakamoto was published in November 2008 together with the Bitcoin concept*48*49. About two months later, in January 2009, the open source Bitcoin v0.1*50 was posted to the Cryptography Mailing List. With the appearance of a usable implementation, the number of users gradually increased*51. At this stage, bitcoins were exchanged over a P2P network that was formed among a small number of community participants, and the value of the bitcoins themselves is believed to have been virtual. Many of the bitcoins generated early on have actually not been used*52.

While Bitcoin once circulated among a closed community of narrow scope, this all changed when its value in the real world was realized and it became possible to exchange it for real currency. At first, there were transactions such as the purchase of pizzas with bitcoins, but it was not possible to exchange them for cash*53. Later, it became possible to trade bitcoins for actual money at exchanges, and stores and websites that allowed payment using bitcoins started to appear*54. This is thought to be because Bitcoin offered substantial benefits to stakeholders such as online retailers, including lower service charges than credit cards, and much faster receipt of funds. Mt.Gox is currently one of the best known exchanges for bitcoins and actual money*55. Looking at the Bitcoin exchange rate*56 for U.S. dollars at Mt.Gox between 2011 and 2013, we can see that their value has risen steadily. This demonstrates that Bitcoin is not limited to users in specific fields such as researchers, and is starting to be accepted by the general public.

Meanwhile, Bitcoin has also been misused in some cases. In January 2011, Bitcoin was adopted as a payment method at the Silk Road Internet market*57 due to the anonymity it provides. At around the same time the Bitcoin exchange rate rose sharply, demonstrating the mania that surrounded it*58. We can surmise that users who wanted to do business transactions in secret started using Bitcoin because they enabled anonymity to be preserved when making payments. The use of Bitcoin subsequently continued to grow, but its exchange rate has fluctuated, plunging at times due to a number of incidents.

■ Technical Description

Viewing Bitcoin from a technological perspective, we can see it has the following characteristics.

- Bitcoin holders remain anonymous.
- No centralized organization for issuing currency exists, and bitcoins are issued by users.
- Bitcoin use involves a process in which data (a transaction) indicating transfer (change of ownership) is created, and validity is ensured through the use of digital signatures. It is possible to detect double spending of the same bitcoins by tracing the chain of signatures associated with these transactions.

Unlike Bitcoin, for cash transfers in the real world, currency is issued based on the reputation of national governments. It is generally also difficult to maintain anonymity for real money transfers over the Internet. The last characteristic of Bitcoin

*48 Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (http://bitcoin.org/bitcoin.pdf).

*49 Satoshi Nakamoto, Bitcoin: P2P Electronic Money System (http://www.bitcoin.co.jp/docs/SatoshiWhitepaper.pdf) (in Japanese). This article is written in Japanese, and is not a machine translation of an English article, so it is believed it was written by a researcher or researchers whose native language is Japanese. Some have indicated that Satoshi Nakamoto is Kyoto University professor Shinichi Mochizuki: Ted Nelson, I Think I Know Who Satoshi Is" (http://www.youtube.com/watch?v=emDJTGTrEm0).

*50 Bitcoin (http://sourceforge.net/projects/bitcoin/).

*51 According to the Original Bitcoin client wiki entry (https://en.bitcoin.it/wiki/Original_Bitcoin_client), Mr. Nakamoto was involved as chief and main developer up to the end of 2010. His whereabouts after that are not known.

*52 Information about the first Bitcoin (https://blockchain.info/ja/block-height/0). There is no evidence of the bitcoins generated in the early stages having been used.

*53 Bitcoin Forum, "Pizza for bitcoins?" (https://bitcointalk.org/index.php?topic=137.0) This is known as an example that shows the value of bitcoins was far lower than it is now.

*54 For example, bitcoinstore (https://www.bitcoinstore.com/), the gift card purchase site gyft (http://www.gyft.com/bitcoin/), and the fashion accessory site Bitfash (http://www.bitfash.com/), etc. LocalBitcoins.com (https://localbitcoins.com/) lets you search for stores where Bitcoins can be purchased and used by entering your location. The EFF accepted Bitcoin donations from an early stage (https://www.eff.org/deeplinks/2011/01/bitcoin-step-toward-censorship-resistant). Regarding methods for exchanging Bitcoins with local currency, the sale of Bitcoin ATMs has begun in Canada (https://robocoinkiosk.com/) China's Baidu also announced they would begin accepting payment via Bitcoin for their service similar to CloudFlare (http://www.coindesk.com/chinese-internet-giant-baidu-starts-accepting-bitcoin/). There is also a restaurant in Japan where bitcoins can be used. This demonstrates that the use of Bitcoin is spreading both geographically and in the diversity of fields involved.

*55 In addition to Mt.Gox (https://www.mtgox.com/), there are other cash exchanges such as coinbase (https://coinbase.com/), Bitstamp (https://www.bitstamp.net/), and BIT-e (https://btc-e.com/). Some exchanges also provide an exchange service for other virtual currencies, such as Litecoin, Primecoin, and Feathercoin.

*56 See the following article for examples of exchange rate fluctuations up to now. Bitcoin.org, "What determines bitcoin's price?" (http://bitcoin.org/en/faq#what-determines-bitcoins-price). At the time of writing this article, the exchange rate varied widely between US$80 per Bitcoin and US$260 per Bitcoin.

*57 Silk Road (https://silkroadvb5piz3r.onion.lu/). The site is currently closed. In October of this year it was hit with allegations regarding issues with the products dealt there, and a large amount of Bitcoins were confiscated.

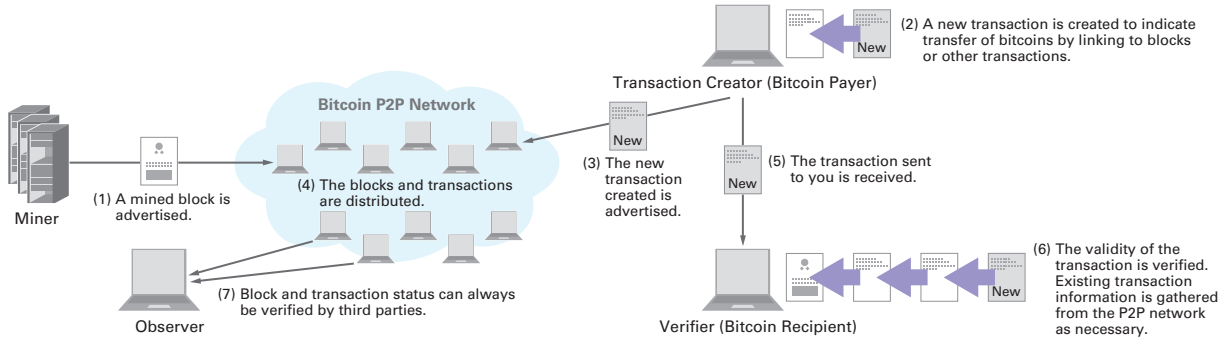
*58 Analysis of Silk Road's Historical Impact on Bitcoin (http://thegenesisblock.com/analysis-silk-roads-historical-impact-bitcoin/).

is it features a system for resolving the issue of electronic data being easy to duplicate. Below, we discuss each of these three characteristics.

First, to handle currency in the digital world, an identifier to indicate the owner is required. For Bitcoin, a unique identifier called a Bitcoin address is allocated. The Bitcoin address is generated from a coin owner's public key. When a Bitcoin user generates a key pair, a Bitcoin address unique to them is automatically allocated. No information that would specify an individual is needed to create this identifier, so it is possible to preserve anonymity. Furthermore, it is possible for an individual to generate multiple Bitcoin addresses, increasing their anonymity. When using bitcoins, information is exchanged over a P2P network, so it is difficult to identify the user.

The second characteristic is that users themselves issue bitcoins. Bitcoin adopts a concept called "proof-of-work", which is implemented using Hashcash*59*60. New coins are issued by performing certain computations, and this computation process is called mining*61. In the beginning it was possible to mine bitcoins using low performance PCs, but now dedicated mining hardware that uses GPUs or ASICs has been developed and is being sold*62. However, these devices are viewed as problematic from an ecological perspective because they require a large amount of electricity, and the profitability of mining drops significantly as the number of miners increases*63. Additionally, the overall volume of currency issued will be decreased every four years. This means it would be difficult to make any money if you were to start participating in mining now.

Last of all is the fact that the safe use of virtual currency is guaranteed. It is easy to duplicate electronic virtual currency, so it is necessary to prevent double spending of the same bitcoins. The transactions that indicate the transfer of bitcoins have a chain-like structure, and are linked to other previous transactions. A given transaction is comprised of information on Inputs and Outputs. Inputs contains pointer information for existing transactions that denotes bitcoins that have been received. Outputs lists the Bitcoin addresses indicating the transferees, as well as the number of bitcoins. All mined information and transactions are circulated among the entire Bitcoin user base, and if any information is missing, it can be obtained from the P2P network. Consequently, when you want to ascertain the flow of currency at the time of trading or at a later date, it is always possible to verify which transaction bitcoins came from and how they were transferred. This system makes it possible to verify that the same bitcoins have not been used multiple times.



- [Mining] The Bitcoin miner advertises the information (block) related to the mined bitcoins over the P2P network.
- [Distribution] Bitcoin users acquire information (blocks) on all bitcoins found, and transaction information or corresponding pointers that indicate the distribution of those bitcoins, from the P2P network.
- [Payment] When paying by Bitcoin, the payer creates a new transaction from the blocks or transactions in their possession, and hands this over to the recipient, while also advertising this fact over the P2P network. Transactions contain information about the Bitcoin recipient and the number of bitcoins. Because digital signatures are used, they cannot be altered.
- [Verification] The Bitcoin recipient uses the blocks, transactions or corresponding pointers in their possession to collect transactions from the P2P network, and obtains the information necessary to verify the validity of the transaction received.
- [Observation] As indicated above, the status of mined bitcoins and their use can be shared, searched, and verified by any user at all times, so the flow of bitcoins can be traced, and double spending of the same blocks/transactions can be detected.

Figure 19: The Bitcoin System

*59 Hashcash (http://hashcash.org/), (https://en.bitcoin.it/wiki/Hashcash).

*60 Proof of work (https://en.bitcoin.it/wiki/Proof_of_work). This indicates a piece of data that was difficult to produce so as to satisfy certain requirements. See *61 for information about the difficulty used with Bitcoin.

*61 Data that records a list of the transactions created during a given period of time is called a block. Blocks are generated approximately every 10 minutes, and each has a given superiority or inferiority. Miners who calculate the best block are allocated new bitcoins. Blocks have a random data area called the nonce. Miners change this nonce to calculate the hash value of the overall block, and compete to find blocks with more zeros at the start of the hash value. Blocks found in this way generate bitcoins that have not been transferred from anyone else. See the Mining wiki entry (https://en.bitcoin.it/wiki/Mining) for more information. The latest status for block chains and the allocation of new bitcoins can also be confirmed on Blockchain (https://blockchain.info/).

*62 See Monarch - Bitcoin Mining Card (http://www.butterflylabs.com/monarch/) as an example.

*63 Bitcoin currency statistics (http://blockchain.info/stats).

The Current Status of Bitcoin

Against such a background, attacks on virtual currency exchanges and account management services rose sharply from the start of this year. In March, money was stolen from BitInstant through the use of DNS hijacking*64. In April, there was a leak of user information from Coinbase, and Mt.Gox experienced outages due to DDoS attacks*65*66. Also in April, there were reports of malware that mines bitcoins on infected users' PCs without their permission spreading via Skype*67. In May, it was discovered that Bitcoin mining code had secretly been inserted into a network game client*68. In August, vulnerabilities were also disclosed in a number of Bitcoin-related applications on Android*69.

Meanwhile, several governments have given an opinion on Bitcoin. The Eastern District of Texas Federal Court, United States, indicated that it considered Bitcoin to be a currency that should be regulated*70. Similarly, Germany also recognized Bitcoin as a currency, and indicated that it should be taxable in its view*71. Meanwhile, the Thai government banned the use of Bitcoin outright*72.

Bitcoin enables transactions with anonymity, and has spread freely across borders without a centralized organization. It is also recognized as a system that is technologically reliable, and it is now on the verge of being accepted by the general public. However, the fact remains that it is also misused. At this point, it is impossible to predict how Bitcoin will be treated in the future. But Bitcoin is a pioneering endeavor, and we believe that similar virtual currencies will continue appearing in different forms.

1.5 Conclusion

This report has provided a summary of security incidents to which IIJ has responded. In this volume, we discussed the PlugX RAT used in targeted attacks, and looked at a series of targeted email attacks. We also examined the Bitcoin virtual currency. 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)
Hiroshi Suzuki, Takahiro Haruyama (1.4.1 The PlugX RAT Used in Targeted Attacks)
Hisao Nashiwa (1.4.2 A Series of Targeted Email Attacks)
Yuji Suga (1.4.3 The Bitcoin Virtual Currency)
Office of Emergency Response and Clearinghouse for Security Information, Service Operation Division, IIJ

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

*64 The website for BitInstant no longer exists, but announcements from the time in question can be viewed on the following Internet Archive page. (http://web.archive.org/web/20130513055208/http://blog.bitinstant.com/blog/2013/3/4/events-of-friday-bitinstant-back-online.html).
*65 Data On Merchant Pages (http://blog.coinbase.com/post/47198421272/data-on-merchant-pages).
*66 Statement Regarding Recent DDoS Attacks and Mitigation (https://www.mtgox.com/pdf/20130424_ddos_statement_and_faq.pdf).
*67 Skypemageddon by bitcoining (http://www.securelist.com/en/blog/208194210/Skypemageddon_by_bitcoining).
*68 See the following official announcement by ESEA for more information. "Bitcoin Fiasco" (http://play.esea.net/index.php?s=news&d=comments&id=12692).
*69 bitcoin.org, Android Security Vulnerability (http://bitcoin.org/en/alert/2013-08-11-android). There have been reports of private key information leaking due to the low entropy of pseudo-random generators. Similar incidents are discussed in IIR Vol.17, under "1.4.1 The Issue of Many Public Keys Used with SSL/TLS and SSH Sharing Private Keys with Other Sites" (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol17_EN.pdf).
*70 The court ruling has not been made public, but can be viewed at the following Internet Archive page (http://ia800904.us.archive.org/35/items/gov.uscourts.txed.146063/gov.uscourts.txed.146063.23.0.pdf).
*71 German politician Frank Schäffler published an exchange with Germany's Federal Ministry of Finance regarding this chain of events. "Bitcoin: Alle Anfragen und Antworten im Volltext" (http://www.frank-schaeffler.de/bitcoin-alle-anfragen-und-antworten-im-volltext/) (in German).
*72 Bitcoin Co. Ltd., "Trading suspended due to Bank of Thailand advisement" (https://bitcoin.co.th/trading-suspended-due-to-bank-of-thailand-advisement/).