The Attackers Behind PlugX

In this report, we present survey results and background information on the attackers behind the PlugX malware used in targeted attacks. We also examine recent trends in DDoS attacks and their countermeasures, and discuss the Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business of the Ministry of Internal Affairs and Communications.

1.1 Introduction

This report summarizes incidents to which IIJ responded, based on general information obtained by IIJ itself related to the stable operation of the Internet, information from observations of incidents, information acquired through our services, and information obtained from companies and organizations with which IIJ has cooperative relationships. This volume covers the period of time from January 1 through March 31, 2014. In this period a number of hacktivism-based attacks were made by Anonymous and other groups, following on from those in the last survey period. DDoS attacks exploiting NTP also occurred frequently, and it was reported that one attack generated a volume of traffic as high as 400 Gbps. Domain hijacking incidents affecting whole countries, such as those where ccTLDs were hijacked, also continued. Additionally, financial damage stemming from the misuse of online banking, which has been on the rise in Japan since last year, is increasing steadily this year. Due to the significant impact of an incident that came to light in the United States at the end of last year, involving the theft of a large amount of information from the POS systems of retailers using malware, there was a great deal of debate regarding countermeasures. As seen above, the Internet continues to experience many security-related incidents.

1.2 Incident Summary

Here, we discuss the IIJ handling and response to incidents that occurred between January 1 and March 31, 2014. Figure 1 shows the distribution of incidents handled during this period*1.

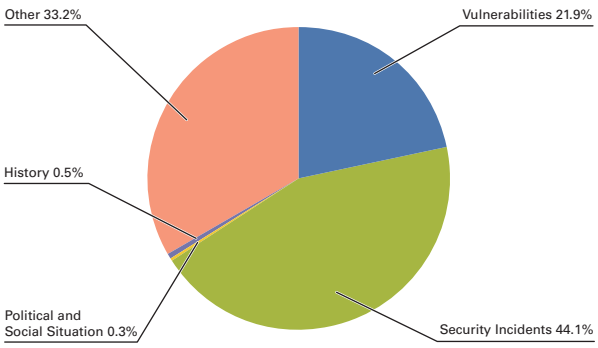


Figure 1: Incident Ratio by Category (January 1 to March 31, 2014)

The Activities of Anonymous and Other Hacktivists

Attacks by hacktivists such as Anonymous continued during this period. DDoS attacks and information leaks occurred at government-related and company sites in a large number of countries stemming from a variety of incidents and causes. In January, a number of government-related sites in Brazil fell victim to Web alterations. Also in January, the website of the Massachusetts Institute of Technology (MIT) was defaced in memory of an activist who committed suicide last year (OpLastResort).

In relation to the situation in Ukraine, there were a number of DDoS attacks on government agencies, leaks of

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

opposition diet member emails and credit card information, and attacks on media websites by groups such as Anonymous in the EU, Ukraine, Russia, and other neighboring countries. Additionally, in March there were DDoS attacks on the North Atlantic Treaty Organization (NATO) thought to be related to this*2.

There were also ongoing attacks by Anonymous and other groups on government and government-related sites in different countries around the world, with the focus on South America and Europe. Unknown attackers claiming affiliation with the Syrian Electronic Army also continued to hijack SNS accounts and deface websites, with affected companies including big names such as Microsoft and Skype.

■ Vulnerabilities and their Handling

During this period fixes were released for Microsoft's Windows*3*4*5*6 and Internet Explorer*7*8. Updates were also made to Adobe Systems' Flash Player, Adobe Reader, Acrobat, and Shockwave Player. A quarterly update was provided for Oracle's Java SE, fixing many vulnerabilities. This update included changes to the security functions, such as limiting the execution of unsigned Java applets to improve security under default settings*9. Several of these vulnerabilities were exploited in the wild before patches were released.

Regarding server applications, a quarterly update was released for a number of Oracle products, including the Oracle database server, fixing many vulnerabilities. A vulnerability in BIND9 DNS servers that caused named to terminate abnormally due to an issue with processing the receipt of DNS queries when operating it as an authoritative DNS server with a DNSSEC signed zone using NSEC3 was also discovered and fixed*10. An issue was also discovered and fixed in NTP, which is used for time synchronization. This issue could lead to DDoS attacks on third parties through the exploitation of a server's administrative functions. A number of attacks exploiting this issue have occurred, and warnings have been issued. See "1.4.2 DrDoS Attacks and Countermeasures" for more information.

In March a regular semi-annual update was released for Cisco Systems' IOS, fixing vulnerabilities including those that could cause system failure*11. An issue that could lead to DDoS attacks on third parties through the exploitation of the Pingback function was also discovered in the WordPress CMS. Attacks in which this issue was actually exploited have occurred*12.

■ Attacks on Web Services

During this period there were ongoing attempts to steal user IDs and passwords, which have occurred frequently since last year. There were also continued incidents of unauthorized login to Web services through identity fraud thought to use lists of the IDs and passwords obtained, as well as malware infections through website alterations.

A large number of incidents in which unauthorized login attempts were made using list-based attacks have occurred at a wide range of sites, including those for ISPs, games, transportation agencies, credit card companies, and SNS. Among these, unauthorized login attempts that targeted frequent flier programs for airline companies resulted in damages such as miles

*2 See the Twitter post of NATO spokesperson Oana Lungescu (@NATOpress) regarding these attacks (https://twitter.com/NATOpress/statuses/445112624578306048).
*3 "Microsoft Security Bulletin MS14-002 - Important: Vulnerability in Windows Kernel Could Allow Elevation of Privilege" (https://technet.microsoft.com/library/security/ms14-002).
*4 "Microsoft Security Bulletin MS14-07 - Critical: Vulnerability in Direct2D Could Allow Remote Code Execution" (https://technet.microsoft.com/library/security/ms14-007).
*5 "Microsoft Security Bulletin MS14-11 - Critical: Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution" (https://technet.microsoft.com/library/security/ms14-011).
*6 "Microsoft Security Bulletin MS14-13 - Critical: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution" (https://technet.microsoft.com/library/security/ms14-013).
*7 "Microsoft Security Bulletin MS14-010 - Critical: Cumulative Security Update for Internet Explorer" (http://technet.microsoft.com/en-us/security/bulletin/ms14-010).
*8 "Microsoft Security Bulletin MS14-012 - Critical: Cumulative Security Update for Internet Explorer" (http://technet.microsoft.com/en-us/security/bulletin/ms14-012).
*9 Oracle, "Developers - Java Content in the Browser — Security Manifest Changes" (http://www.java.com/en/download/faq/signed_code.xml).
*10 Internet Systems Consortium, "CVE-2014-0591: A Crafted Query Against an NSEC3-signed Zone Can Crash BIND" (https://kb.isc.org/article/AA-01078).
*11 "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" (http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar14.html).
*12 See the following Krebs on Security blog post for more information about these attacks. "Blogs of War: Don't Be Cannon Fodder" (http://krebsonsecurity.com/2014/03/blogs-of-war-dont-be-cannon-fodder/).

January Incidents

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

V **1st:** A backdoor in a number of Cisco Linksys devices that could allow the router to be reset remotely or the admin password to be obtained were discovered, and a researcher released details.
See the researcher's following GitHub for more information. "elvanderb/TCP-32764" (https://github.com/elvanderb/TCP-32764).

S **2nd:** US-CERT issued a warning regarding malware that infects POS terminals, which caused information leaks at major retailer companies that came to light in December.
US-CERT, "Alert (TA14-002A) Malware Targeting Point of Sale Systems" (http://www.us-cert.gov/ncas/alerts/TA14-002A).

S **4th:** A number of online games were targeted in DDoS attacks by unknown entities, causing service outages, etc. It has been indicated that these attacks may have targeted a specific user.

S **6th:** The Japan Atomic Energy Agency announced that a PC used for clerical processing at the Monju fast-breeder reactor had been infected by a virus, and information may have leaked.
"Concerning Potential Information Leaks due to a Computer Virus Infection" (http://www.jaea.go.jp/02/press2013/p14010601/index.html) (in Japanese).

S **6th:** U.S. company Yahoo! announced that over the year-end and New Year period some of the advertisements distributed on its European site had redirected users to malware from malicious sites.
See the following TrendLabs Security Intelligence Blog post for more information. "Malicious Yahoo Ads – Preventable With Patching, Security Solutions" (http://blog.trendmicro.com/trendlabs-security-intelligence/malicious-yahoo-ads-preventable-with-patching-security-solutions/).

S **8th:** In South Korea, it was discovered that a total of 85 million pieces of credit card information had been leaked from three major credit card companies by an employee of a credit bureau that had contracts with the credit card companies.

S **11th:** A service outage lasting two days occurred at the Dropbox online storage service due to issues during maintenance.
See the following official Dropbox blog post for more information about this outage. "Outage post-mortem" (https://tech.dropbox.com/2014/01/outage-post-mortem/).

V **15th:** A warning was issued due to the possibility of the monlist function in ntpd causing a DoS.
US-CERT, "Alert (TA14-013A) NTP Amplification Attacks Using CVE-2013-5211" (http://www.us-cert.gov/ncas/alerts/TA14-013A).

V **15th:** Microsoft published their Security Bulletin Summary for January 2014, and released four important updates including MS14-002.
"Microsoft Security Bulletin Summary for January 2014" (http://technet.microsoft.com/en-us/security/bulletin/ms14-jan).

V **15th:** A number of vulnerabilities in Adobe Reader and Acrobat that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB14-01 Security updates available for Adobe Reader and Acrobat" (http://helpx.adobe.com/security/products/acrobat/apsb14-01.html).

V **15th:** A number of vulnerabilities in Adobe Flash Player that could allow arbitrary code execution were discovered and fixed.
"Security updates available for Adobe Flash Player" (http://helpx.adobe.com/security/products/flash-player/apsb14-02.html).

V **15th:** Oracle released their quarterly scheduled update for a number of products including Oracle, fixing a total of 144 vulnerabilities, including 36 in Java SE.
"Oracle Critical Patch Update Advisory - January 2014" (http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html).

S **15th:** Symantec announced that the website of a major publisher in Japan had been altered, and users had been redirected to malware from a malicious site using Toolkit.
See the following Symantec Security Response blog post for more information. "Popular Japanese Publisher's Website led to Gongda Exploit Kit" (http://www.symantec.com/connect/blogs/popular-japanese-publisher-s-website-led-gongda-exploit-kit).

O **23rd:** Security-related companies issued warnings regarding malware infections that fraudulently used the update function of the GOM Player video playback software.
This is thought to have been the cause of a virus infection incident at the Japan Atomic Energy Agency that was announced on January 6. See the following announcement from South Korea's GRETECH JAPAN Corp for more information. "Apology and report on survey results regarding malware (virus) infections" (http://www.gomplayer.jp/player/notice/view.html?intSeq=300) (in Japanese).

O **29th:** An old root certificate for GMO GlobalSign expired, causing issues such as connection failure and warnings appearing on the client side if the updated certificate was not installed.
GlobalSign, "Expiration of old GlobalSign 2014 Root CA Certificate" (https://support.globalsign.com/customer/portal/articles/1426272-expiration-of-old-globalsign-2014-root-ca-certificate).

O **30th:** IPA published their "Targeted Attack Email Trends and Case Studies <2013>" technical report, which analyzed targeted attack email between October 2012 and December 2013.
"Targeted Attack Email Trends and Case Studies <2013>" (http://www.ipa.go.jp/security/technicalwatch/20140130.html) (in Japanese).

S **31st:** Some accounts on U.S. company Yahoo!'s Yahoo! Mail service were affected by incidents of unauthorized login stemming from list-based attacks.
Yahoo! Inc., "Important Security Update for Yahoo Mail Users" (http://yahoo.tumblr.com/post/75083532312/important-security-update-for-yahoo-mail-users).

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

*Dates are in Japan Standard Time

and other gift points being exchanged without authorization. Issues with the specifications of some of the affected sites were pointed out earlier, such as users being able to set passwords with too few characters. As shown here, unauthorized access incidents continue to occur frequently, and ongoing vigilance is required.

During this period there were also many website alterations, as well as incidents in which users were redirected to malware from altered websites. These also occurred on SNS-related sites and the websites of a number of publishing and broadcasting-related companies, as well as websites for transport agencies and financial institutions. Malware infection activity via drive-by download took place on the sites users were redirected to, involving the use of several vulnerabilities, including zero-day ones. These Web alterations have also occurred on the websites of well-known companies, so it will be necessary to remain vigilant in the future.

■ Attacks on ccTLD

Numerous attacks on domain registries including ccTLD continue to occur, along with associated domain hijackings and information leaks. In January, .me domains for Montenegro were accessed without authorization by an unknown entity, and approximately 3,500 domains were hijacked. The management tools for the MarkMonitor domain management service that manages domains for Google, Yahoo!, Amazon, and Facebook among others were accessed without authorization by someone claiming affiliation with the Syrian Electronic Army, leading to the information for some of these domains being overwritten.

In March, a Venezuelan ISP advertised the Google Public DNS (8.8.8.8) routing information, affecting traffic to the Google Public DNS on networks in Venezuela and Brazil. Regarding Google Public DNS, in Turkey it was discovered that communications were being carried out with servers other than the original ones, and it was pointed out that this may be due to government censorship*13. Additionally, in Turkey access to other sites such as Twitter and YouTube has been blocked, suggesting that government restrictions on the Internet are intensifying.

■ Bitcoin

As transactions using the Bitcoin*14 virtual currency become more widespread, a variety of incidents are occurring. During the current survey period, Bitcoin exchange Mt. Gox announced in February that they were temporarily suspending transactions due to a technical problem occurring. Several days later, another Bitcoin exchange, Bitstamp, also temporarily suspended transactions due to problems. It was announced that these exchanges had been targeted by DoS attacks exploiting an issue with Bitcoin transaction malleability*15. This issue could have interfered with transactions or made double spending possible through overwriting and advertising the unique transaction IDs used for Bitcoin transactions. Bitstamp resumed transactions after seemingly dealing with the issue, but Mt. Gox was apparently made bankrupt due to liabilities of about 6.5 billion yen in this incident when bitcoins in their possession were stolen, and they filed for protection under Japan's Civil Rehabilitation Act. However, because it had been pointed out before the collapse that their transactions lacked transparency, their application was rejected and bankruptcy procedures started on account of their business operations not being clear*16.

It has been revealed that although Mt. Gox had been made aware of this issue in 2011, they ignored it and did not make fixes to their system. Furthermore, it was announced that some of the assets said to have been stolen were discovered in an old-format Bitcoin wallet*17. A survey published by a third party also pointed out that of the 740,000 XBT of bitcoins affected by this issue, those stolen due to this issue may amount to only approximately 386 XBT.

There has also been a rash of other attacks on virtual currency exchanges and account management services, involving many DDoS attacks on websites, as well as server compromises in which bitcoins and site account information were stolen. Despite reports from a number of U.S. news outlets that Satoshi Nakamoto, believed to be the creator of Bitcoin, had been found, the individual identified denied he was the person in question. Lively discussions regarding the handling of Bitcoin are currently taking place all over the world. In March, the Japanese cabinet declared that it does not consider Bitcoin a currency.

*13 Google Online Security Blog. "Google's Public DNS intercepted in Turkey" (http://googleonlinesecurity.blogspot.jp/2014/03/googles-public-dns-intercepted-in-turkey.html).

*14 See Vol.21 (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol21_EN.pdf) of this report under "1.4.3 The Bitcoin Virtual Currency" for more information about Bitcoin.

*15 Bitstamp, "BITCOIN WITHDRAWAL PROCESSING SUSPENDED" (http://www.bitstamp.net/article/bitcoin-withdraws-suspended/).

*16 MtGox Co., Ltd., "Announcement of Commencement of Bankruptcy Proceedings" (http://www.mtgox.com/img/pdf/20140424_announce_qa_en.pdf).

*17 MtGox Co., Ltd., "We inform you as follows with regard to the balance of bitcoins (BTC) held by MtGox Co., Ltd." (http://www.mtgox.com/img/pdf/20140320-btc-announce.pdf).

February Incidents

1 **S** **3rd:** An incident occurred in which a member-oriented website for an airline company was accessed without authorization, and miles exchanged for e-commerce site points.

2 **S** **3rd:** The Kavli Institute for the Physics and Mathematics of the Universe announced its supercomputer system had been accessed without authorization from outside. Unauthorized access related to the system compromised in this incident was also confirmed at external research institutions, including the National Astronomical Observatory of Japan with which joint research was being carried out, so measures were taken at these institutions.
See the following announcement from Kavli Institute for the Physics and Mathematics of the Universe (Kavli IPMU) for more information.
"Regarding unauthorized access to Kavli Institute for the Physics and Mathematics of the Universe research computer"
(http://www.ipmu.jp/ja/node/1831) (in Japanese).

3 4

5 **V** **5th:** A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB14-08: Security updates available for Adobe Flash Player" (http://helpx.adobe.com/security/products/flash-player/apsb14-08.html).

6 **O** **5th:** The Ministry of Economy, Trade and Industry and the JPCERT Coordination Center held the "Control System Security Conference 2014" for evaluating security improvements to control systems by presenting domestic and international technological trends for control systems.
JPCERT Coordination Center, "Information about the Control System Security Conference 2014"
(https://www.jpcert.or.jp/event/ics-conference2014.html) (in Japanese).

7 8 9

10 **S** **6th:** The National Cancer Center announced that two computers in the National Cancer Center Hospital East had been infected with a virus, and patient and other information may have leaked.
See the following National Cancer Center announcement for more information. "Regarding computer virus infections stemming from a video playback software update program in the National Cancer Center Hospital East" (http://www.ncc.go.jp/jp/information/20140206.html) (in Japanese).

11 **S** **7th:** The Mt. Gox Bitcoin exchange temporarily suspended the payout of bitcoins to fix a technical issue. They subsequently filed for bankruptcy protection under the Civil Rehabilitation Act on February 28 after becoming insolvent due to the draining of their Bitcoin and bank deposits in a cyber attack.

12 **S** **12th:** Account withdrawals were temporarily suspended at Bitcoin exchanges such as Mt. Gox and Bitstamp after they were targeted in attacks that interfered with transactions by exploiting transaction malleability. This caused the Bitcoin to dollar exchange rate to temporarily drop sharply.
A research team at the University of Zurich also investigated Mt. Gox to verify this issue, and countered that the impact of this issue was limited. Christian Decker and Professor Roger Wattenhofer, "Bitcoin Transaction Malleability and MtGox" (http://arxiv.org/pdf/1403.6676v1.pdf).

13 **V** **12th:** Microsoft published their Security Bulletin Summary for February 2014, and released four critical updates including MS14-007, MS14-010, and MS14-011, as well as three important updates.
"Microsoft Security Bulletin Summary for February 2014" (http://technet.microsoft.com/en-us/security/bulletin/ms14-feb).

14 **V** **12th:** A number of vulnerabilities in Adobe Shockwave Player that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB14-06: Security update available for Adobe Shockwave Player" (http://helpx.adobe.com/security/products/shockwave/apsb14-06.html).

15 16

17 **O** **12th:** The opening session of the trial for the suspect arrested in the "Remote Control Virus" incident that occurred two years ago was held at the Tokyo District Court.

18 **O** **13th:** The U.S. National Institute of Standards and Technology (NIST) published its "Framework for Improving Critical Infrastructure Cybersecurity," which serves as an index for implementing information security measures at organizations and companies in the field of critical infrastructure.
NIST, "NIST Releases Cybersecurity Framework Version 1.0" (http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm).

19 **V** **17th:** It was reported that there was a vulnerability in the CGI script of a number of U.S. Cisco Linksys routers, and this had been exploited in multiple infections of a malware known as TheMoon. See the following U.S. SANS ISC InfoSec Diary post for more information.
"Linksys Worm 'TheMoon' Summary: What we know so far"
(https://isc.sans.edu/forums/diary/Linksys+Worm+TheMoon+Summary+What+we+know+so+far/17633).

20 **O** **17th:** CODE BLUE, an international information security conference originating in Japan, was held over two days.
See the following official site for CODE BLUE for more information (http://www.codeblue.jp/en-index.html).

21 22 **S** **18th:** Measures were taken after it was discovered that advertisements accompanying search site results were being exploited to redirect users to a number of fraudulent financial institution sites.
See the following announcement for more information about this incident. "Follow-up regarding the exploitation of advertisements accompanying search results" (http://advertisingblog.yahoo.co.jp/2014/02/post_33.html) (in Japanese).

23 24 **V** **20th:** Microsoft released an advisory due to an unpatched vulnerability in Internet Explorer that could allow remote code execution when exploited. It was confirmed that this vulnerability had already been exploited at the time of the announcement.
"Microsoft Security Advisory (2934088): Vulnerability in Internet Explorer Could Allow Remote Code Execution"
(http://technet.microsoft.com/en-us/security/advisory/2934088).

25 26 **V** **21st:** A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"Security updates available for Adobe Flash Player" (http://helpx.adobe.com/security/products/flash-player/apsb14-07.html).

27 28 **S** **24th:** Hatena alerted its users to change their password and check registered details due to the possibility of external unauthorized login to the services they provide.
Hatena Co., Ltd., "Check your password and registered details to prevent unauthorized login"
(http://hatena.g.hatena.ne.jp/hatena/20140224/1393211701) (in Japanese).

O **27th:** IPA published "Improper release of information by the growing number of Internet-connected devices and measures to prevent it," which summarized new threats due to the Internet connection of office devices and home appliances, as well as procedures for confirming whether information is being made public inadvertently.
"IPA Technical Watch 'Improper release of information by the growing number of Internet-connected devices and measures to prevent it'"
(http://www.ipa.go.jp/security/technicalwatch/20140227.html) (in Japanese).

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

*Dates are in Japan Standard Time

■ Attacks on Business Systems

In incidents involving the leak of credit card information for customers of major retailers in the United States in November of last year, a subsequent investigation determined that 40 million sets of credit card information and 70 million sets of customer data may have been stolen. It also came to light that special POS malware that targeted credit card readers and registers had been used to carry out this theft. Additionally, it has been announced that a number of other companies were targeted in similar attacks, including high-end department stores*18.

The malware used in these attacks is designed to steal information by targeting the moment that credit card and other data encrypted for a transaction is decrypted on the register when processing payment. It then sent the stolen data to external servers*19.

Because IDs loaned to traders of affected business operators were stolen and used maliciously in these incidents, it is believed that attacks were carried out after compromising the internal networks of these business operators. It is said that the equipment management systems and customer information management systems were linked by networks at these business operators, and insufficient information security measures are thought to have contributed to the large scale of the information leaks.

Because business terminals such as industrial systems and POS systems are sometimes not directly connected to the Internet, they are not properly managed in many cases, including security measures and software updates not being implemented in contrast to PCs used at companies. It is thought that attacks on business systems such as POS terminals will continue due to these conditions, so caution is required.

■ Attacks Via Legitimate Software

In January, it was announced that a virus had been found on a PC shared by employees at the Japan Atomic Energy Agency's Monju fast-breeder reactor*20. In February it was reported that two PCs at the National Cancer Center Hospital East were also infected by a virus*21. These virus infections were caused by exploiting a legitimate update function in video playback software. In these incidents, an update server used by legitimate software installed by users had been accessed without authorization and altered. This caused users to be redirected to a third-party site not intended by the update server when performing a software update, where malware presented as an update program for the corresponding software could be downloaded and executed*22.

Other examples of legitimate software management systems being exploited include system failures on a large number of PCs at multiple broadcasters and financial institutions in South Korea in March 2013. In these incidents, the update management server (patch management system) within affected companies was accessed without authorization, and malware that crashes systems was distributed to PCs throughout the company*23. There have also been recent cases in which legitimate apps or browser extensions were acquired and embedded with unauthorized functions which were then distributed as updates*24.

To deal with issues such as these, it will be necessary to implement systems for verifying whether or not updates to installed software are legitimate, and increase security for software update servers within companies.

*18 Krebs on Security, "Hackers Steal Card Data from Neiman Marcus" (http://krebsonsecurity.com/2014/01/hackers-steal-card-data-from-neiman-marcus/).

*19 See the following Kaspersky Lab blog post for more information. "RAM Scrapers and Other Point-of-Sale Malware" (http://blog.kaspersky.com/ram-scrapers-and-other-point-of-sale-malware/).

*20 The Japan Atomic Energy Agency, "Concerning Potential Information Leaks due to a Computer Virus Infection" (http://www.jaea.go.jp/02/press2013/p14010601/index.html) (in Japanese).

*21 National Cancer Center, "Regarding computer virus infections stemming from a video playback software update program in the National Cancer Center Hospital East" (http://www.ncc.go.jp/jp/information/20140206.html) (in Japanese).

*22 Gretech Japan Corporation, "Apology and report on survey results regarding malware (virus) infections" (http://www.gomplayer.jp/player/notice/view.html?intSeq=300&page=1) (in Japanese).

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

*24 Regarding this incident, the aftermath of actually selling a Chrome extension with 30,000 users was reported on the blog of its author, Amit Agarwal. "Selling a Google Chrome Extension is Easy but Monetizing is Tricky" (http://www.labnol.org/internet/sold-chrome-extension/28377/).

March Incidents

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

V **5th:** Security researchers at the French Institute for Research in Computer Science and Automation (INRIA) disclosed a new method for attacking TLS that may have had client certificates stolen through a MITM attack.
See the following announcement for more information. "Triple Handshakes Considered Harmful Breaking and Fixing Authentication over TLS" (https://secure-resumption.com/).

V **6th:** A vulnerability in GnuTLS that could allow MITM attacks through the impersonation of legitimate websites due to an issue with certificate validation under specific circumstances was discovered and fixed.
US-CERT, "GnuTLS Releases Security Update" (http://www.us-cert.gov/ncas/current-activity/2014/03/05/GnuTLS-Releases-Security-Update).

O **7th:** In response to a Memorandum on Questions regarding Bitcoin, the Japanese government reached a cabinet decision and announced that it does not consider Bitcoin a currency in Japan.
House of Councilors, "Memorandum on Questions Regarding Bitcoin" (http://www.sangiin.go.jp/japanese/joho1/kousei/syuisyo/186/meisai/m186028.htm) (in Japanese).

七 **10th:** It was announced that unauthorized login incidents had occurred at a member-oriented website for another airline company, and miles were exchanged for other points.

O **10th:** IPA announced a Web application version of the "AppGoat" vulnerability learning tool, which enables vulnerability discovery methods and countermeasures to be studied systematically in a practical format. This version added new study topics and exercises for patching vulnerabilities.
"The AppGoat Vulnerability Hands-On Learning Tool" (http://www.ipa.go.jp/security/vuln/appgoat/index.html) (in Japanese).

V **12th:** Microsoft published their Security Bulletin Summary for March 2014, and released two critical updates including MS14-012 and MS14-013, as well as three important updates.
"Microsoft Security Bulletin Summary for March 2014" (http://technet.microsoft.com/en-us/security/bulletin/ms14-mar).

V **12th:** A number of vulnerabilities in Adobe Flash Player including those that could allow information leaks were discovered and fixed.
"APSB14-08: Security updates available for Adobe Flash Player" (http://helpx.adobe.com/security/products/flash-player/apsb14-08.html).

V **12th:** A number of vulnerabilities in Adobe Shockwave Player that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB14-08: Security updates available for Adobe Flash Player" (http://helpx.adobe.com/security/products/flash-player/apsb14-08.html).

七 **12th:** A large-scale DDoS attack occurred. This exploited the Pingback function that notifies users that one of their posts has been linked to on the WordPress CMS.
Sucuri Blog, "More Than 162,000 WordPress Sites Used for Distributed Denial of Service Attack" (http://blog.sucuri.net/2014/03/more-than-162000-wordpress-sites-used-for-distributed-denial-of-service-attack.html).

V **13th:** It was announced that the Samsung Galaxy series included a function that could allow the execution of remote file operations.
See the following Free Software Foundation blog post for more information. "Replicant developers find and close Samsung Galaxy backdoor" (http://www.fsf.org/blogs/community/replicant-developers-find-and-close-samsung-galaxy-backdoor).

七 **17th:** A temporary BGP hijacking of the Google Public DNS route occurred in Brazil and Venezuela.
See the following BGP Mon tweet for more information about this incident. (https://twitter.com/bgpmon/status/445266642616868864/photo/1).

V **18th:** An issue that allowed a caller's number to be misrepresented was found in the IP telephony function of a messaging app, attracting a lot of attention.

O **18th:** Approximately 100 personnel from all government ministries, the National Information Security Center, and critical infrastructure providers came together to undergo training in collecting and sharing information across ministries and conducting emergency responses.
National Information Security Center, "Large-scale government cyber attack countermeasure training by participants from across all government agencies - [3/18 Training] -" (http://www.nisc.go.jp/active/kihon/pdf/318.pdf) (in Japanese).

V **19th:** A number of vulnerabilities in the Apache HTTP Server were discovered and fixed, including those that could allow DoS attacks.
The Apache Software Foundation, "Apache HTTP Server 2.2.27 Released" (http://www.apache.org/dist/httpd/Announcement2.2.html).

O **19th:** The Full Disclosure mailing list established in 2002 that had been used as a forum for disclosing and discussing vulnerability information was closed. On March 25, another administrator resumed the mailing list under the same name.
seclists.org, "Administrivia: The End" (http://seclists.org/fulldisclosure/2014/Mar/332). seclists.org, "Administrivia: A Fresh Start" (http://seclists.org/fulldisclosure/2014/Mar/333).

O **20th:** The Internet Content Safety Association announced that from April 1 they would launch an initiative to prevent the distribution of child pornography using file sharing software by sending email to corresponding users.
"Countermeasures for the distribution of child pornography using file sharing software" (http://www.netsafety.or.jp/p2p/index.html) (in Japanese).

V **25th:** Microsoft published an advisory confirming that targeted attacks had been made by exploiting an unpatched vulnerability in Microsoft Word that could allow arbitrary code execution.
"Vulnerability in Microsoft Word Could Allow Remote Code Execution" (https://technet.microsoft.com/library/security/2953095)

O **26th:** The Ministry of Defense formed a new Cyber Defense Unit for responding to cyber attack threats that continue to grow more sophisticated and complex.
Ministry of Defense, "Regarding the formation of a new Cyber Defense Unit" (http://www.mod.go.jp/j/press/news/2014/03/25d.html) (in Japanese).

O **27th:** The National Police Agency announced details of the status of cyber crime arrests made in 2013. A record 8,113 arrests were made, which was 10.6% higher than the previous year.
National Police Agency, "Regarding the status of cyber crime arrests made within 2013" (https://www.npa.go.jp/cyber/statics/h25/pdf01-2.pdf) (in Japanese).

O **31st:** IPA published "10 Major Security Threats for the Year 2014."
"10 Major Security Threats for the Year 2014." (https://www.ipa.go.jp/security/vuln/10threats2014.html).

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

*Dates are in Japan Standard Time

■ Government Agency Initiatives

Government agency initiatives included the "38th Assembly of the Information Security Policy Council" held in January. Here, a basic policy was put together regarding the understanding and evaluation of data based on the performance index for the "Cyber Security Strategy"*25 that was decided in June of last year, as well as "Cyber Security 2013"*26 that determined the efforts of each ministry for FY2013. There was also discussion of a unification model for information security measures at government agencies. Furthermore, to cultivate a better understanding of cyberspace threats that continue to grow in complexity and sophistication, as well as their countermeasures, it has been decided that the first work day in February will be designated "Cyber Security Day," placing the focus on initiatives that contribute to the safety of cyberspace. The "Overall Strategy Promotion Committee for IT Use and Application Security" was also held in February. Here, the overall and strategic promotion of information security policies that take into account future IT utilization was discussed. On March 18, training was implemented for information gathering and sharing between the National Information Security Center, various government agencies, and critical infrastructure providers, in addition to emergency response training of CYMAT personnel, based on a hypothetical situation in which a number of government agencies had been targeted by simultaneous cyber attacks.

■ Other

In January ICANN approved "TOKYO" and "NAGOYA" as new gTLDs. "OKINAWA" was also approved in March*27. This was due to the new gTLD approval process*28 that ICANN has been working on since January 2012. Currently close to 2,000 new gTLD applications have been made from around the world, and new gTLDs are likely to appear one after another in the future.

The National Police Agency released "Status of Incidents of Illegal Remittance Related to Internet Banking in 2013"*29. This reported that 1,315 of these incidents occurred during 2013, reaching a total of approximately 1,406,000,000 yen in damages, which was higher than ever before. The number of incidents also rose sharply in June and beyond in particular, with techniques used to obtain IDs and passwords including a large number of cases in which users were prompted to enter their details on a fraudulent screen displayed by a virus to steal them. From November onward there were reports of many incidents of redirection to phishing sites through email.

In February the president of a company that ran a proxy server and two others were arrested on suspicion of violating the Act on Prohibition of Unauthorized Computer Access by accessing an ISP using IDs and passwords obtained without authorization. Because the proxy server run by this company did not record logs and was not able to track users, it is thought to have been used for unauthorized remittances via Internet banking, as well as the sending of targeted attack emails.

Also in February, there was the opening session of the trial of a suspect charged with forcible obstruction of business, who was arrested in relation to a series of incidents linked to the "Remote Control Virus" that made headlines last year. The suspect is maintaining his innocence.

In March, the Ministry of Internal Affairs and Communications published a summary of the November 2013 results for its periodic tally/estimate of Internet traffic, which it carries out with the cooperation of ISPs, Internet exchanges, and researchers*30. According to these results, the estimated total download traffic of broadband service subscribers was approximately 2.6 Tbps as of November 2013, which is an increase of 35.6% compared to the same month the previous year. Additionally, total upload traffic was estimated at approximately 834 Gbps, which is also a 25.2% increase over the same month the previous year.

*25 National Information Security Center, "Information Security Policy Council - 35th Assembly" (June 10, 2013) (http://www.nisc.go.jp/conference/seisaku/index.html#seisaku35) (in Japanese).

*26 National Information Security Center, "Information Security Policy Council - 36th Assembly" (June 27, 2013) (http://www.nisc.go.jp/conference/seisaku/index.html#seisaku36) (in Japanese).

*27 See the following ICANN "DELEGATED STRINGS" (http://newgtlds.icann.org/en/program-status/delegated-strings) for more information about the approved gTLDs.

*28 ICANN, "New gTLDs Update: Applications Accepted Today; New Guidebook Posted; Financial Assistance for Qualifying Applicants" (http://www.icann.org/en/news/announcements/announcement-11jan12-en.htm).

*29 National Police Agency, "Status of Incidents of Illegal Remittance Related to Internet Banking in 2013" (http://www.npa.go.jp/cyber/pdf/H260131_banking.pdf) (in Japanese).

*30 Ministry of Internal Affairs and Communications, "Summary/Estimate of Internet Traffic in Japan" (http://www.soumu.go.jp/menu_news/s-news/01kiban04_02000077.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 utilize advanced knowledge such as that of vulnerabilities, but rather cause large volumes of unnecessary traffic to overwhelm network bandwidth or server processes for the purpose of hindering services.

■ Direct Observations

Figure 2 shows the circumstances of DDoS attacks handled by the IIJ DDoS Protection Service between January 1 and March 31, 2014. This information shows traffic anomalies judged to be attacks based on IIJ DDoS Protection Service standards. IIJ also responds to other DDoS attacks, but these incidents are excluded from the figure due to the difficulty in accurately ascertaining the facts of each situation.

There are many methods that can be used to carry out a DDoS attack, and the capacity of the environment attacked (bandwidth and server performance) will largely determine the degree of impact. Figure 2 categorizes DDoS attacks into three types: attacks on bandwidth capacity*31, attacks on servers*32, 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 495 DDoS attacks. This averages to 5.5 attacks per day, indicating almost no change in the average daily number of attacks compared to our prior report. Server attacks accounted for 61% of all incidents, while compound attacks accounted for 20.8%, and bandwidth capacity attacks 18.2%.

The largest attack observed during the period under study was classified as a compound attack, and resulted in 2.86 Gbps of bandwidth using up to 601,000 pps packets. Of all attacks, 90.5% ended within 30 minutes of commencement, 9.5% lasted between 30 minutes and 24 hours, and none lasted over 24 hours. The longest sustained attack was a server attack that lasted for 10 hours and 55 minutes. The NTP-based attacks that garnered a lot of attention during this survey period peaked with an attack that generated 1.8 Gbps of traffic using up to 517,000 pps packets.

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*33 and botnet*34 usage as the method for conducting DDoS attacks.

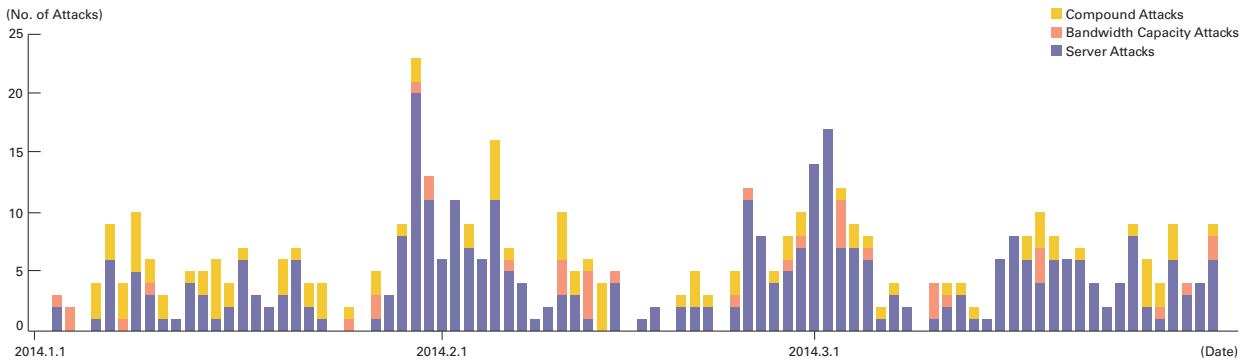


Figure 2: Trends in DDoS Attacks

*31 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.

*32 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.

*33 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.

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

■ Backscatter Observations

Next we present our observations of DDoS attack backscatter using the honeypots*35 set up by the MITF, a malware activity observation project operated by IIJ*36. By monitoring backscatter it is possible to detect some of the DDoS attacks occurring on external networks as a third party without any interposition.

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

The port most commonly targeted by the DDoS attacks observed was the 80/TCP port used for Web services, accounting for 33.1% of the total during the target period. Attacks were also observed on 53/UDP used for DNS, 3389/TCP used for remote desktop, and 22/TCP used for SSH, as well as 8010/TCP and 8000/TCP, which are normally not used.

Looking at the origin of backscatter thought to indicate IP addresses targeted by DDoS by country in Figure 3, the United States accounted for the largest ratio at 15.2%. Chile and Germany followed at 9.6% and 9.0%, respectively. Continuing on from the last survey, many Chilean IP addresses were observed. This was due to the fact that packets from multiple IP addresses targeting 445/TCP on multiple honeypots had been observed a total of over 72,000 times during the current survey period.

Regarding particularly large numbers of backscatter packets observed, attacks on Web servers (80/TCP) targeting a U.S. hosting provider were observed between January 2 and 4, a German hosting provider on February 18, and IP addresses in Belize owned by a Hong Kong hosting provider between February 23 and 24. On January 23 we observed attacks on 8400/TCP targeting servers in China, and on March 24 there were attacks on 8000/TCP targeting a Russian site in Germany. We also observed attacks on 8010/TCP targeting the IP addresses of an ISP in the British Virgin Islands between March 26 and 27.

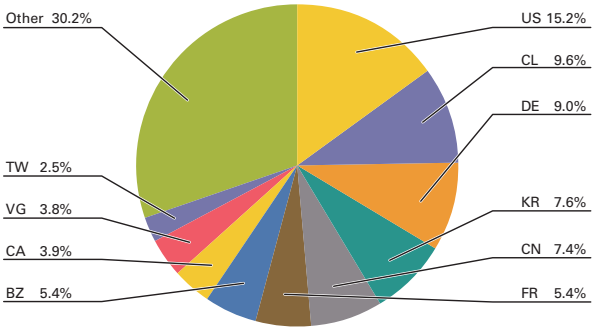


Figure 3: Distribution of DDoS Attack Targets According to Backscatter Observations (by Country, Entire Period under Study)

During the current survey period we noted an increase in DNS (53/UDP) backscatter from February 4. Most of these packets were thought to be the result of querying domain names including random character strings to a large number of IP addresses. Although it is not clear whether

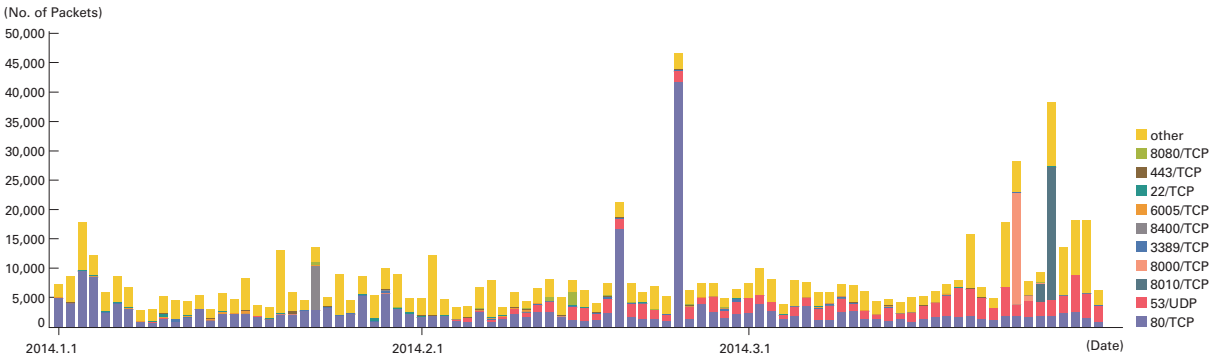


Figure 4: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)

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

*36 The mechanism and limitations of this observation method, as well as some of the results of IIJ's observations, are presented in Vol.8 on this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol08_EN.pdf) under "1.4.2 Observations on Backscatter Caused by DDoS Attacks."

directly-related to these packets, an alert regarding the increasing dangers of cache poisoning attacks was issued by JPRS on April 15*37. It will be necessary to double check DNS server configuration and keep an eye on future trends.

On January 4 attacks on servers related to online games were observed, and these were part of attacks that were reported on a number of game and technology-related news sites.

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the MITF*38, a malware activity observation project operated by IIJ. The MITF uses honeypots*39 connected to the Internet in a manner similar to general users in order to observe communications arriving over the Internet. Most appear to be communications by malware selecting a target at random, or scans attempting to locate a target for attack.

■ Status of Random Communications

Figure 5 shows the distribution of sender's IP addresses by country for communications coming into the honeypots between January 1 and March 31, 2014. Figure 6 shows trends in the total volumes (incoming packets). The MITF has set up numerous honeypots for the purpose of observation. We have taken the average per honeypot, showing the trends for incoming packet types (top ten) over 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.

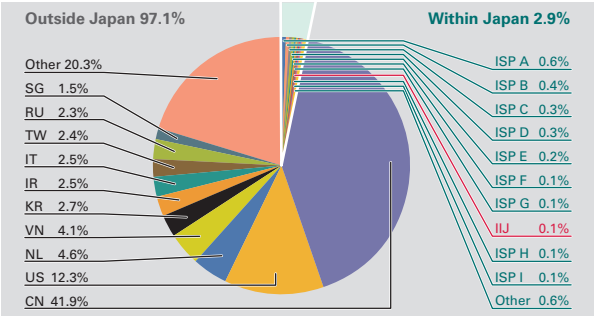


Figure 5: Sender Distribution (by Country, Entire Period under Study)

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, 80/TCP used for HTTP, ICMP echo requests, 53/UDP used for DNS, and 23/TCP used for Telnet.

Communications thought to be SSH dictionary attacks also occurred sporadically during the current period. For example, communications that occurred on March 20 was from Singapore and South Korea, and communications that occurred between March 24 and 25 were from IP addresses

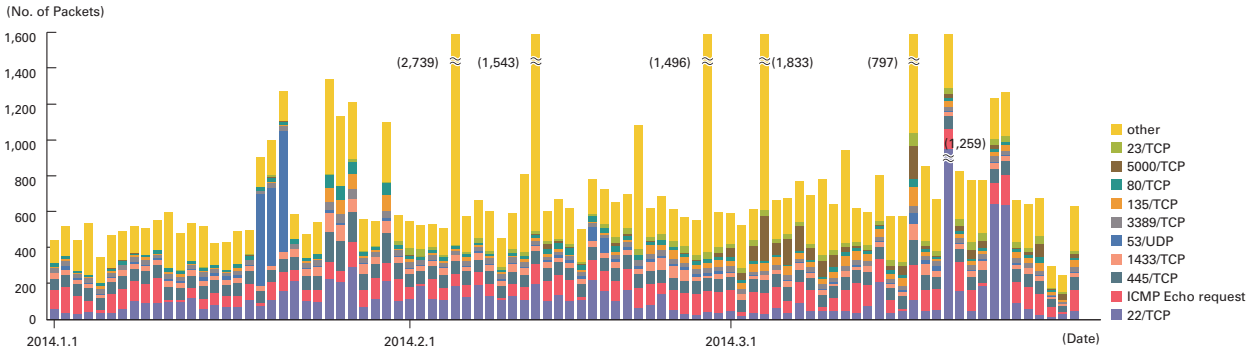


Figure 6: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

*37 JPRS, "(Critical) Regarding the double checking of DNS server configurations in light of the increasing danger of cache poisoning attacks" (http://jprs.jp/tech/security/2014-04-15-portrandomization.html) (in Japanese).

*38 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.

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

allocated to Italy. Additionally, between mid-January and February the volume of SSH communications was higher compared to the previous survey period. This was mainly due to an increase in communications from IP addresses allocated to China.

Between January 19 and 21, there was an increase in DNS communications. Examining the details of communications, we learned an IP address allocated to the Netherlands had been making repeated ANY record query attempts targeting 28 domains. After investigating further, from the comparatively large size of responses from each of the 28 domains, IIJ believes the attacker had been attempting to make DNS Amp attacks on these IP addresses by spoofing the Dutch IP address and sending repeated queries*40.

Extensive repeated scanning behavior was carried out from an IP address allocated to Vietnam on February 5, and from an IP address allocated to China on February 12 and 27, as well as March 4. This targeted TCP ports between 1000 and 9999, as well as some UDP ports.

■ Scanning and Attacks Targeting Embedded Devices (NAS, DVR)

During the current survey period, scanning behavior targeting 5000/TCP began to increase from mid-February, and rose dramatically in March. Figure 7 shows trends (average value per honeypot) in the total volume (incoming packets) for the source IP addresses of 5000/TCP communications arriving at the honeypots.

This is believed to be scanning behavior or attacks on vulnerabilities in Synology NAS or Hikvision DVR (Digital Video Recorder) products. Vulnerabilities that could allow arbitrary code execution on these products were discovered in 2013, and exploits have also already been disclosed. Incidents involving similar events have also been noted a number of times by the National Police Agency and on the SANS ISC blog*41, and there have been reports of programs thought to be malware that were not originally present being detected in products believed to have been attacked.

■ 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 in the number of acquired specimens show the total number of specimens acquired per day*42, while the number of unique specimens is the number of specimen variants categorized according to their digest of a

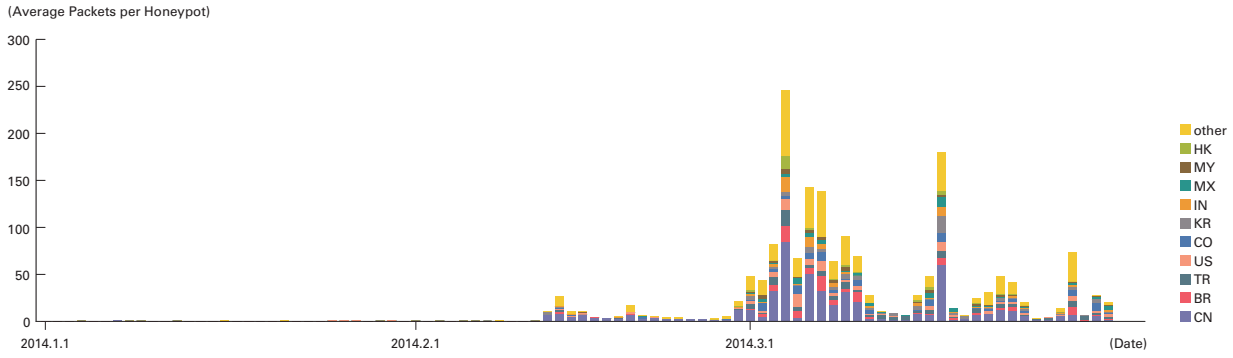


Figure 7: Country-by-Country Trends in the Source IP Addresses of 5000/TCP Communications Arriving at Honeypots (Average by Honeypot)

*40 Because the honeypots reject DNS queries, amplified responses are not delivered to the corresponding IP address.

*41 See the following National Police Agency announcement. "Regarding the sharp increase in access targeting port 5000/TCP believed to be scanning for NAS with vulnerabilities" (http://www.npa.go.jp/cyberpolice/detect/pdf/20140305.pdf) (in Japanese). SANS ISC reported honeypot data and malware survey results regarding this phenomena in the following four blog entries. "TCP/5000 - The OTHER UPNP Port" (https://isc.sans.edu/diary/TCP5000+-+The+OTHER+UPNP+Port/17763). "Port 5000 traffic and snort signature" (https://isc.sans.edu/diary/Port+5000+traffic+and+snort+signature/17771). "Let's Finally 'Nail' This Port 5000 Traffic - Synology owners needed." (https://isc.sans.edu/diary/Let%27s+Finally+%22Nail%22+This+Port+5000+Traffic+-+Synology+owners+needed./17859). "More Device Malware: This is why your DVR attacked my Synology Disk Station (and now with Bitcoin Miner!)" (https://isc.sans.edu/diary/More+Device+Malware%3A+This+is+why+your+DVR+attacked+my+Synology+Disk+Station+%28and+now+with+Bitcoin+Miner!%29/17879).

*42 This indicates the malware acquired by honeypots.

hash function*43. 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, 114 specimens were acquired per day during the period under study, representing 21 different malware. The "Other" category was higher on January 25 and March 17. These were due to an increase in the Allaple*44 family of malware from IP addresses allocated to Brazil and Taiwan, respectively. Allaple is known as polymorphic malware, and shows up more prominently in Figure 10.

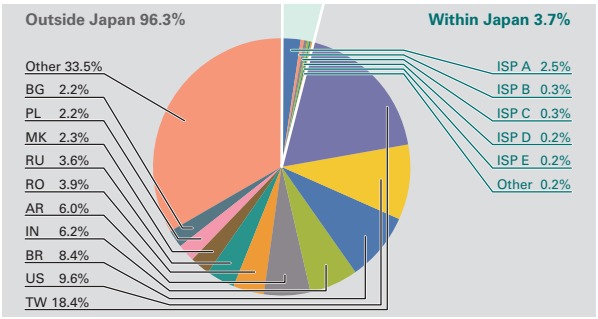


Figure 8: Distribution of the Total Number of Malware Specimens Acquired

After investigating the undetected specimens more closely, worms*45 were observed from IP addresses allocated to a number of countries, including India. Additionally, about 71% of undetected specimens were text format. Because many of these text format specimens were HTML 404 or 403 error responses from Web servers, we believe this was due to infection behavior of malware such as old worms continuing despite the closure of download sites that newly-infected PCs access to download malware.

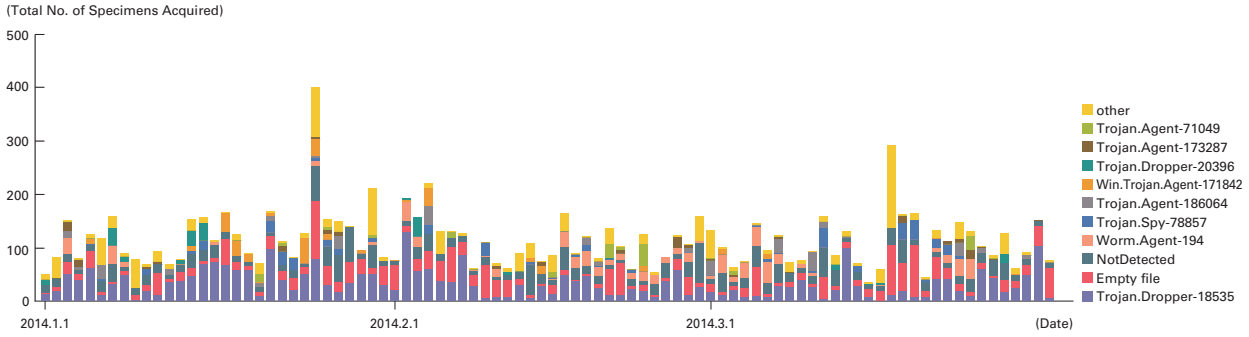


Figure 9: Trends in the Total Number of Malware Specimens Acquired (Excluding Conficker)

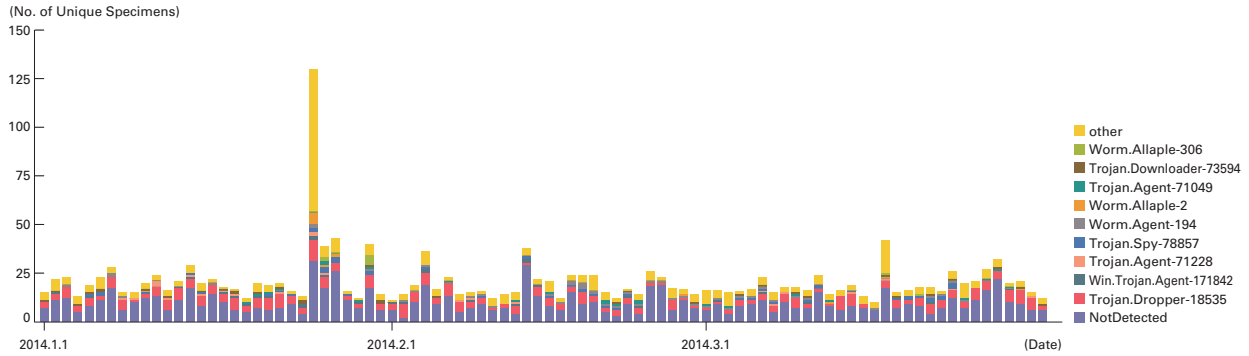


Figure 10: Trends in the Number of Unique Specimens (Excluding Conficker)

*43 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.

*44 Win32/Allaple (http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?name=Win32%2fAllaple).

*45 WORM_ATAK (http://about-threats.trendmicro.com/archiveMalware.aspx?language=jp&name=WORM_ATAK.D).

Under the MITF's independent analysis, during the current period under observation 92.4% of malware specimens acquired were worms, 4.6% were bots, and 3.0% were downloaders. In addition, the MITF confirmed the presence of 16 botnet C&C servers*46 and 7 malware distribution sites.

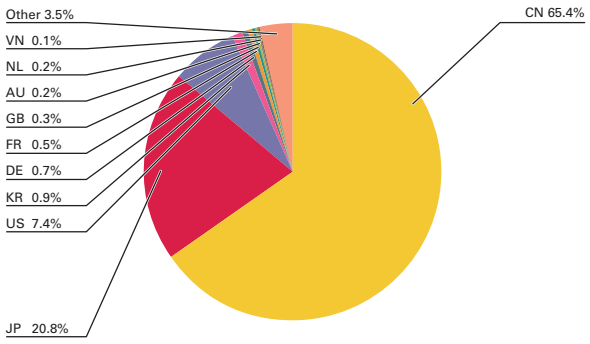
■ Conficker Activity

Including Conficker, an average of 35,739 specimens were acquired per day during the period covered by this report, representing 787 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 decreased slightly by approximately 2% compared to the previous survey period. Unique specimens increased by about 4%. According to the observations of the Conficker Working Group*47, as of March 31, 2014, a total of 1,277,911 unique IP addresses are infected. This is a drop of approximately 40% compared to the 3.2 million PCs observed in November 2011, but it demonstrates that infections are still widespread.

1.3.3 SQL Injection Attacks

Of the types of different Web server attacks, IIJ conducts ongoing surveys related to SQL injection attacks*48. 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 January 1 and March 31, 2014. Figure 12 shows trends in the numbers of attacks. These are a summary of attacks detected by signatures on the IIJ Managed IPS Service.



China was the source for 65.4% of attacks observed, while Japan and the United States accounted for 20.8% and 7.4%, respectively, with other countries following in order. There was a significant increase in the number of SQL injection attacks on Web servers compared to the previous report. However, this was due to a number of large-scale attacks from China that occurred during the current survey period, and when these are excluded there is little change in detection trends.

Figure 11: Distribution of SQL Injection Attacks by Source

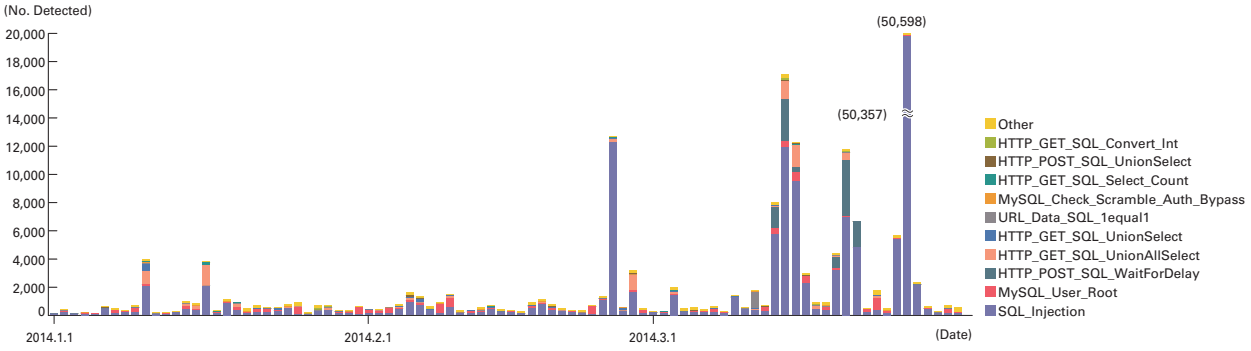


Figure 12: Trends in SQL Injection Attacks (by Day, by Attack Type)

*46 An abbreviation of Command & Control Server. A server that provides commands to a botnet consisting of a large number of bots.
*47 Conficker Working Group Observations (http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking).
*48 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.

During this period, attacks from a specific attack source in China directed at specific targets took place on February 25. Between March 13 and 15, there were attacks from a number of other attack sources in China on other specific targets. Attacks including those from the same specific attack sources in China on the same specific targets were also made between March 19 and 21. Between March 25 and 27, there were large-scale attacks from another specific attack source in China on another specific target. These attacks are thought to have been attempts to find vulnerabilities on Web servers.

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

1.3.4 Website Alterations

Here we indicate the status of website alterations as surveyed through the MITF Web crawler (client honeypot)*49 (Figure 13). This Web crawler accesses tens of thousands of websites on a daily basis, with a focus on well-known and popular sites in Japan. We also add new target sites on a regular basis. Websites with temporary spikes in access numbers are also included in our observations. By surveying websites thought to be viewed frequently by typical users in Japan, it is easier to speculate on trends regarding fluctuations in the number of altered sites, as well as the vulnerabilities exploited and malware distributed.

Between January and mid-February 2014, the Sweet Orange Exploit Kit and Ramayana Exploit Pack (also known as DatkaChef or the DotCacheF Exploit Kit) were used in the majority of attacks. This is a trend that has continued since the end of last year, and most of the websites altered and used in attacks were comparatively small in scale, such as those for small and medium-sized enterprises, or online shops From exploit kit trends, we believe these attacks mainly targeted vulnerabilities such as those in older versions of JRE.

Meanwhile, from the second half of February onward, the total number of attacks declined sharply, and those using the Sweet Orange Exploit Kit were no longer observed at all. Instead, attacks using the Infinity Exploit Kit (also known as Red Kit v2 or Goon Exploit Kit) increased, and we observed attacks exploiting a vulnerability in Microsoft Internet Explorer (CVE-2014-0322) that was disclosed on February 20, for which a patch was not available at the time. During this period, there were a number of website alterations at comparatively well-known major companies, and in most of these cases the attacks exploited the aforementioned vulnerability in Internet Explorer.

In late March, a converging trend was seen in attacks, with drive-by download attacks estimated to be on the decline in Japan. However, this trend may abruptly change based on the intentions of attackers, so website operators and visitors must continue to be careful.

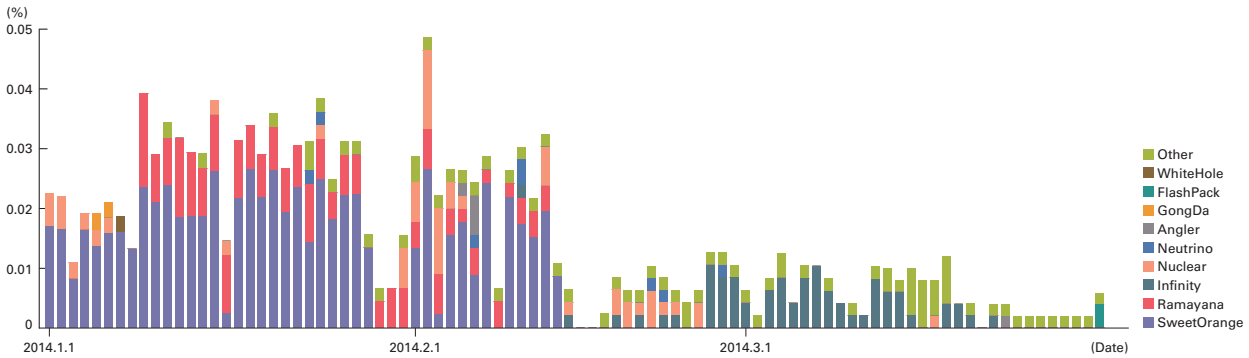


Figure 13: Rate of Drive-By Download Incidence When Viewing Websites (%) (by Exploit Kit)

* Covers several tens of thousands of sites in Japan.
  In recent years, exploit kits have been configured to change attack details and whether or not attacks are made based on the client system environment or session information, source address attributes, and the quota achievement status of factors such as number of attacks. This means that results can vary at times depending on the trial environment and timing of crawler access.
* Because the Web crawler was not operating between February 15 and 16, no attacks were detected.

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

1.4 Focused Research

Incidents occurring over the Internet change in type and scope from one minute to the next. Accordingly, IIJ works toward implementing countermeasures by continuing to perform independent surveys and analyses of prevalent incidents. Here we will present information from the surveys we have undertaken during this period, including discussion of the attackers behind PlugX, a look at DrDoS attacks and their countermeasures, and an explanation of the Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business.

1.4.1 The Attackers Behind PlugX

In March 2014, IIJ gave a presentation at Black Hat Asia 2014*50 regarding PlugX*51. The presentation involved finding points in common between PlugX specimens and classifying them into groups by extracting and analyzing C&C server config information from PlugX specimens, and investigating which kinds of targeted attack groups were behind each PlugX group. In this section, we share these results, and also explain why we carried out this investigation.

■ PlugX Variants

PlugX is an RAT*52 discovered in March 2012 that has frequently been used in targeted attacks. IIJ has confirmed the existence of three broadly-defined types of PlugX variant at the time of writing. Here we will refer to these as Type I, II, and III. Type I is the specimen type that has been found most often since the discovery of PlugX, and we previously discussed it in Vol.21 of this report*51. Type II is a new variant of PlugX*53 as reported in the IIJ-SECT Security Diary. This variant was discovered in the third quarter of 2013. This is significantly more advanced than Type I, and includes changes such as the elimination of the "GULP" signature that was a characteristic of PlugX, and implementation of a function for passing through proxies with basic authentication. Type III has existed since before Type I, and it has been reported that as a previous incarnation of PlugX*54 it was used in past incidents. Although the commands for processing instructions from C&C servers and communication characteristics are almost identical to Type I and II, its code characteristics are significantly different, and it has stronger anti-analysis functions. It also continues to be updated now, like Type I and II.

■ Extracting Config Information from Each PlugX Specimen

Each PlugX variant has extremely different code characteristics. Consequently, IIJ created extraction scripts corresponding to each variant, making it possible to extract useful config information (the C&C server and auto start details such as the service name, and registry values) from all variants. Because we were able to standardize a lot of the processing for Type I and II, we implemented this as a single Immunity Debugger*55 script. Because we could not identify PlugX code for Type III in the process memory due to its anti-analysis functions such as obfuscation, we implemented this as an IDAPython*56 script that performs semi-automatic extraction. Using these scripts, we attempted to extract config information from PlugX specimens with 150 unique hash values. Of these, 27 specimens were demo versions*57 that did not contain config information. As a result, we used the remaining 123 specimens for classification.

*50 Black Hat (https://www.blackhat.com/) is the world's largest IT security conference. It is held each year, mainly in the United States, Europe, and Asia. IIJ gave a presentation at Black Hat Asia 2014, which was held in the Asian region.

*51 PlugX is discussed in detail in IIR Vol.21 (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol21_EN.pdf).

*52 An abbreviation of Remote Administration Tool, which is a type of malware used mainly to control hosts remotely. Because this type of malware is a starting point for the targeted attacks that are carried out, IIJ keeps a watchful eye on it and conducts regular analysis. Some experts define it as an abbreviation for Remote Access Tool or Remote Access Trojan.

*53 IIJ Security Diary "New Types of PlugX Appear" (https://sect.iij.ad.jp/d/2013/11/197093.html) (in Japanese). This touches upon each of the Type II and Type III variants.

*54 According to "SK Hack by an Advanced Persistent Threat" (https://www.commandfive.com/papers/C5_APT_SKHack.pdf), it was reported that a RAT called Destory RAT was used in an attack in 2011. IIJ has confirmed that this is almost identical to PlugX Type III.

*55 Immunity Debugger is a debugger for Windows provided by Immunity, Inc. (https://www.immunityinc.com/products-immdbg.shtml). It was created based on OllyDbg, and features Python extensions. Plug-ins and scripts can be written in Python.

*56 IDAPython is a Python extension for automating processes in the IDA Pro (https://www.hex-rays.com/products/ida/) disassembler and debugger provided by Hex-Rays.

*57 See the following site for more information about the demo version of PlugX: "An Analysis of PlugX" (http://lastline.com/labs/plugx). Because config information is often padded with "XXXX" strings in the demo version, it is not possible to extract this information. However, we also confirmed some specimens have config information without padding even though the demo version flag is set. Specimens such as these are included in our analysis.

■ PlugX Classification

Figure 14 illustrates the classification techniques used for PlugX. After extracting config information using the scripts mentioned earlier, we find the points in common for each specimen and classify them.

In the first stage, we classified specimens based on the service name. Upon infection PlugX registers itself as a service or adds a value to the Run key in the registry so it can continue to operate even if the infected host is rebooted. We grouped those with distinguishing values*58. In the second stage, we carried out further grouping based on C&C server information (FQDN, IP address*59, domain name, and email address of domain owner) and debug strings in the code*60.

Table 1 shows the groups that emerged after repeating these processes. We were able to classify two-thirds of all PlugX specimens into seven groups. Furthermore, in this case we define a group as having at least four specimens.

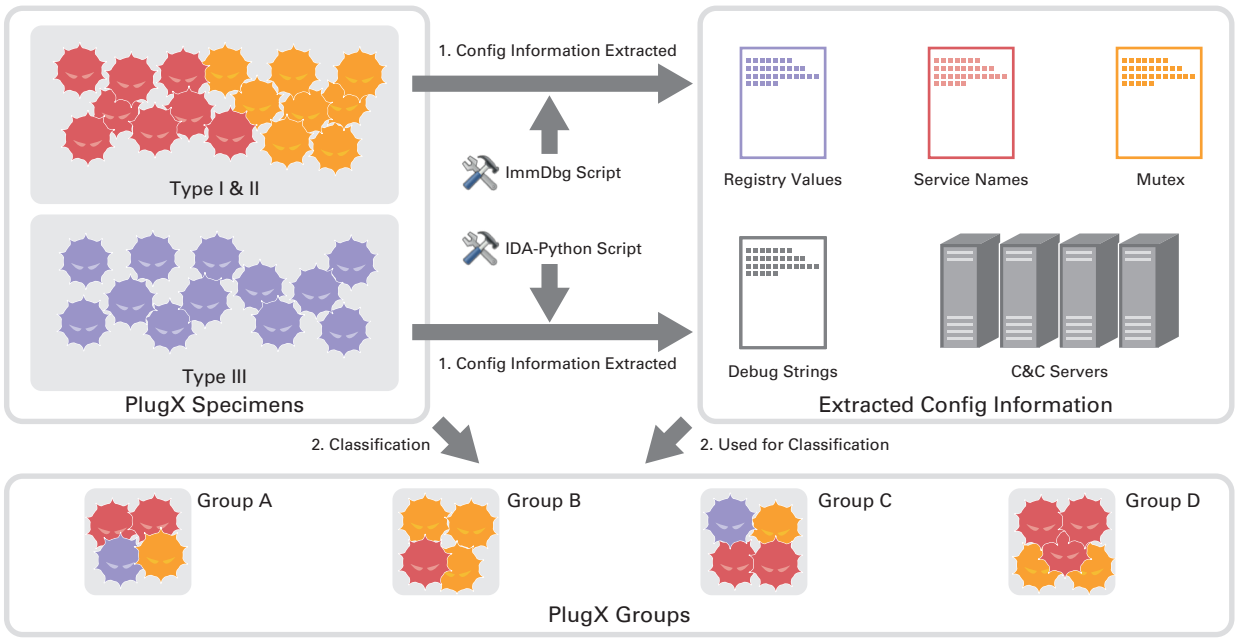
Table 1: PlugX Specimen Classification Results

PlugX Group Name	Type I	Type II	Type III	Group Total	
*Sys	15	0	5	20	About two-thirds of all specimens (67%)
*Http	12	3	0	15	
Starter	13	7	4	24	
Graphedt	8	0	0	8	
WS	6	1	0	7	
360	4	0	0	4	
cochin	0	0	4	4	
- (Others)	30	8	3	41 *Note	

* Note: 8 of these specimens were confirmed to be associated with a targeted attack group.

■ Comparison with Known Targeted Attacker Groups

Last of all, we investigated whether the PlugX groups generated in the previous steps were associated with known targeted attacker groups. Specifically, we looked at whether the specimens written in external reports for targeted attacks had matching hash values or C&C server information. Figure 15 summarizes these relationships. In



1. Config information is extracted from each PlugX specimen using a script corresponding to its type.
2. Based on the extracted config information, specimens with config information values that match or correlate with others are grouped together for classification.

Figure 14: PlugX Classification Method

*58 When grouping by service name, default values such as "SxS," "XXX," and "TVT" were excluded from the grouping key. Meanwhile, most of the specimens classified as being in the same group by service name had matching or similar C&C server information. For this reason, it is considered likely that individual service names are used for a certain period of time or are set by each attacker.

*59 Including the IP address resolved from the FQDN.

*60 Most PlugX specimens are still currently under active development. Perhaps as a result of this, there are many specimens compiled with debugging enabled. When an error occurs during some kind of processing in PlugX, there is a routine that records the details of the error including version details that indicate which version the error occurred in, as well as path information along with Chinese-language characters. Because many different patterns exist for this path information string, we believe this information can also be used to indicate when the same attacker was responsible. The following website introduces many examples of the debug strings used. "CASSIDIAN CyberSecurity Blog PlugX: some uncovered points" (http://blog.cassidiancybersecurity.com/post/2014/01/plugx-some-uncovered-points.html?2014/01/plugx-some-uncovered-points.html).

this survey, we learned that five of the seven PlugX groups identified were connected to an existing incident of some sort. The survey results pointed to the fact that four of these five groups in particular were associated with an attacker group called APT1*61. This either indicates that many attackers using PlugX belong to APT1, or at least different attacker groups are sharing infrastructure. Furthermore, we discovered that eight of the PlugX specimens we could not classify into groups were associated with some form of known targeted attacker group, such as APT1 or Winnti*62.

■ Considering New Countermeasure Techniques

This survey was carried out using PlugX as an example. Because targeted attacks are aimed at a small number of specific organizations, it is often difficult to see the big picture, such as the attacker's intentions, the scale of the group, and the tools and infrastructure used in attacks. Because each organization can only obtain a limited number of specimens, they tend to implement countermeasures by relying on information gained from a small number of specimens. On the other hand, when a large number of specimens are collected it may shed new light on matters as we have here, such as identifying that many PlugX groups are associated with APT1. Once this is known, it could be possible to implement multifaceted countermeasures corresponding to the progress of the attack, such as detection and countermeasures based on the characteristics of the attack methods or attack tools an APT1 attacker uses after compromising an organization via a RAT.

During the presentation at Black Hat Asia, in addition to the presentation materials and scripts for extracting config information, we also handed out a correlation diagram*63 showing links between each PlugX specimen and known targeted attacker groups. This is in an image format called SVG. While an SVG is an image, it actually uses XML format, and by analyzing this it is possible to extract all the information disclosed here such as the C&C servers, etc. That means this data could be used for countermeasures with exit controls.

Wider and more comprehensive sharing of information by each organization affected in targeted attacks will lead to countermeasures becoming available. IIJ will continue to conduct analysis and surveys like those mentioned here, and actively disclose information to promote measures for combating targeted attacks.

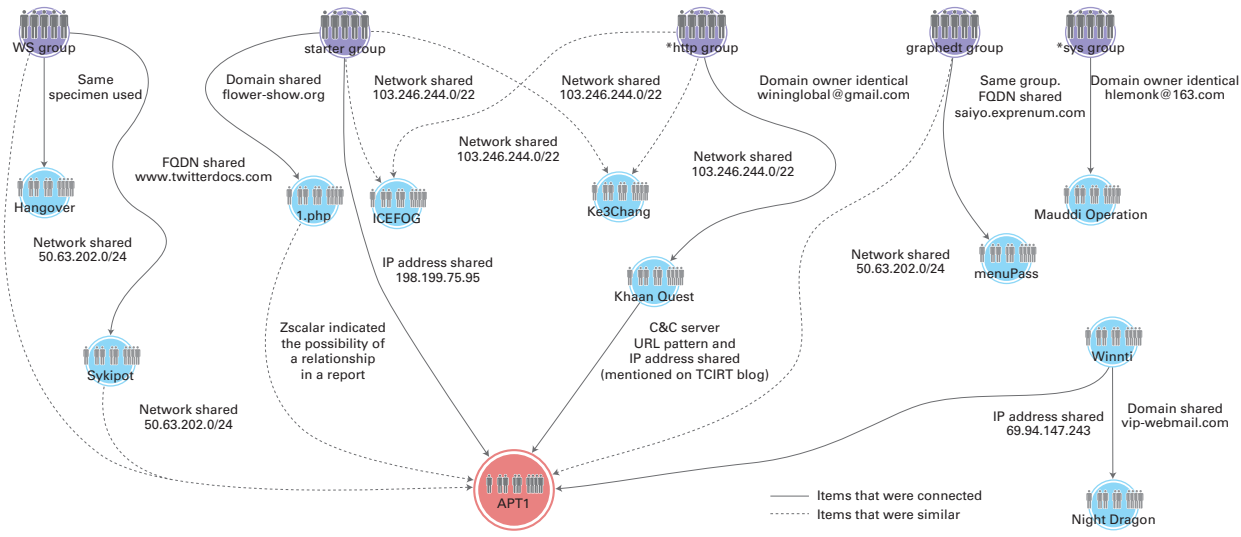


Figure 15: Correlation Between PlugX Groups and Targeted Attacker Groups

*61 APT1 is a group carrying out targeted attacks that was reported by Mandiant (http://intelreport.mandiant.com/).

*62 Winnti is a targeted attack aimed at the game industry that was reported by Kaspersky Lab (https://www.securelist.com/en/downloads/vlpdfs/winnti-more-than-just-a-game-130410.pdf).

*63 The presentation materials, extraction script, and correlation chart can be obtained from the Black Hat archive site (https://www.blackhat.com/asia-14/archives.html#Haruyama). Updated versions of the scripts are also available from the following link (http://takahiroharuyama.github.io/blog/2014/03/27/id-slash-idapython-scripts-extracting-plugx-configs/).

1.4.2 DrDoS Attacks and Countermeasures

In March 2013, DDoS attacks that exploited DNS open resolvers became an issue*64. These attacks exploited DNS cache servers that allow recursive queries from external sources, sending queries with the source IP address spoofed to appear as the attack target's IP address to flood the target server with responses as a DDoS attack.

In around October, NTP-based DDoS attacks were observed*65, and in December a report regarding NTP-based DDoS attacks was posted on the blog of U.S. company Symantec*66. In these NTP-based DDoS attacks, the monlist management function in NTP was exploited to carry out DDoS attacks by sending queries with the source IP address spoofed, just like with the DNS-based attacks. In January 2014, a number of organizations in Japan such as the JPCERT Coordination Center also issued alerts due to the high likelihood of this problem being exploited in DDoS attacks*67. A number of incidents in which these attacks caused damages or were used as stepping stones have actually been confirmed. Furthermore, a number of NTP-based DDoS attacks have been made by an unknown entity on game-related sites in the United States and Europe since around December 2013. These peaked at 80 Gbps, and were reported on the blog of U.S. DDoS protection provider Staminus*68. Cloud provider CloudFlare also reported that attacks of up to 400 Gbps had been made on their customers*69, and ArborNetworks noted NTP-based traffic of up to 800 Gbps in observation data they obtained from a number of ISP networks*70.

These are called Distributed Reflection Denial of Service attacks (DrDoS attacks), and they have become an issue due to the ease of carrying them out and the significant potential impact though amplification. In this section we explain DrDoS attacks and also look into countermeasures.

■ The DrDoS Attack Mechanism

As their name suggests, DrDoS attacks are those that exploit responses to certain communications (reflection). UDP services such as DNS and NTP are often exploited due to UDP being a connectionless protocol, which makes it easy to attack. Because attacks appear to be coming from the IP address of a vulnerable device that is used as a stepping stone, the victim does not know who the real attacker is. This means that even if communications from the attack source are blocked, it is possible to find a new stepping stone and continue the attack, so measures taken on the victim's side may not always deal with the root cause of the attack.

Furthermore, DrDoS attacks take advantage of the fact that the data volume of responses to queries is greater than attacking a target directly, amplifying the scale of an attack by several times to several dozen times. For example, with DNS it is theoretically possible to amplify by up to 70 times*71. The NTP monlist function exploited in the attacks that have recently become a problem can lead to data approximately 200 times larger than the original query being sent if the theoretical maximum value was returned. This demonstrates that the amplification rate is extremely high for NTP*72. DrDoS attacks use this to generate a volume of traffic that exceeds the target's bandwidth capacity.

*64 See Vol.21 of this report under "2. Internet Operation - DNS Open Resolver Issues" (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol21_EN.pdf) for more information about the issue of DNS open resolvers.

*65 This can be confirmed in a report from the CERT team of Lithuanian research and education institution LITNET. LITNET CERT, "NTP DoS reflection attacks" (https://cert.litnet.lt/en/docs/ntp-distributed-reflection-dos-attacks).

*66 Symantec Cyber Readiness & Response Blog, "Hackers Spend Christmas Break Launching Large Scale NTP-Reflection Attacks" (http://www.symantec.com/connect/blogs/hackers-spend-christmas-break-launching-large-scale-ntp-reflection-attacks).

*67 JVN, "JVNVU#96176042 Issues with NTP being used as a stepping stone in DDoS attacks" (http://jvn.jp/vu/JVNVU96176042/) (in Japanese).

*68 Staminus Communications, "Mitigating 80 Gbps Attacks – NTP Amplification Attacks on the Rise" (https://blog.staminus.net/mitigating-80-gbps-attacks-ntp-amplification-attacks-on-the-rise).

*69 CloudFlare, "Technical Details Behind a 400 Gbps NTP Amplification DDoS Attack" (http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack).

*70 ArborNetworks, "NTP attacks continue – a quick look at traffic over the past few months" (http://www.arbornetworks.com/asert/2014/03/ntp-attacks-continue-a-quick-look-at-traffic-over-the-past-few-months/).

*71 Because amplification is actually limited by the cache DNS server configuration, etc., the maximum is between 8 times and 40 times.

*72 An alert regarding the amplification of protocols used in attacks has also been issued in a CERT/CC advisory. "Alert (TA14-017A) UDP-based Amplification Attacks" (https://www.us-cert.gov/ncas/alerts/TA14-017A).

■ NTP-Based DrDoS Attacks and Their Impact

The potential for DrDoS attacks via the NTP monlist command that are now an issue was pointed out by a developer community involved in the implementation of NTP in 2010, and in May of that year the issue was fixed*73. However, this fix was only applied to the Development version, and the Stable version remained unpatched at 4.2.6p5. Consequently, this fix was not applied to devices such as routers and UNIX-based OSes that used certain ntpd implementations*74.

Figure 16 illustrates the NTP-based DrDoS attacks that have now become an issue. In some NTP implementations such as ntpd, a monlist command that returns a list of client IP addresses it is referenced from is implemented for management purposes. If a device such as a router or server that responds to external queries is in place, responses are returned to the attack target by sending queries with the source spoofed to appear as the attack target's IP address. Attackers perform attacks by directing communications like this to a large number of devices. Because ntpd has lists of up to 600 client IP addresses that it is referenced from, it is thought that in these attacks the attacker remotely sent successive queries using spoofed IP addresses to boost the list to its maximum size, and then spoofed the actual attack target to make the attack.

Regarding this NTP issue, there are two points to take note of regarding NTP servers. The first is the fact that they may be exploited as stepping stones in DrDoS attacks. When used as a stepping stone in these attacks, you are both a victim and perpetrator of the attack at the same time. The other point is the potential for information leaks. This issue involves the monlist command, which is a management function that returns a list of client IP addresses it is referenced from. For this reason, responding to external queries could lead to information such as the IP addresses of clients on the network used by the NTP server being leaked externally.

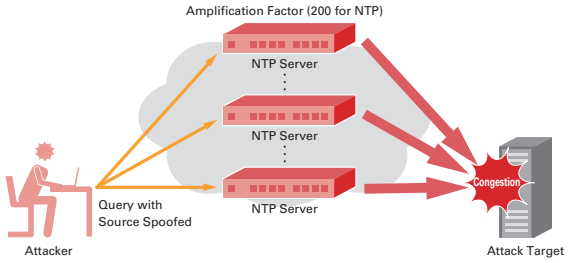


Figure 16: DrDoS Attack Overview (NTP)

■ Honeypot Observation Status

Figure 17 shows the sender's IP addresses classified by country for NTP (123/UDP) communications that reached our honeypots between early October last year and late March this year. We can see from this that communications were carried out from a source in Germany from mid-November. The figure also indicates that communications have occurred on an ongoing basis since the disclosure of vulnerability information by CERT/CC and others in mid-January*75. Looking at these results by country, the United States was the most common at 36.8%, followed by the Netherlands at 25% and Germany at 14.3%, demonstrating

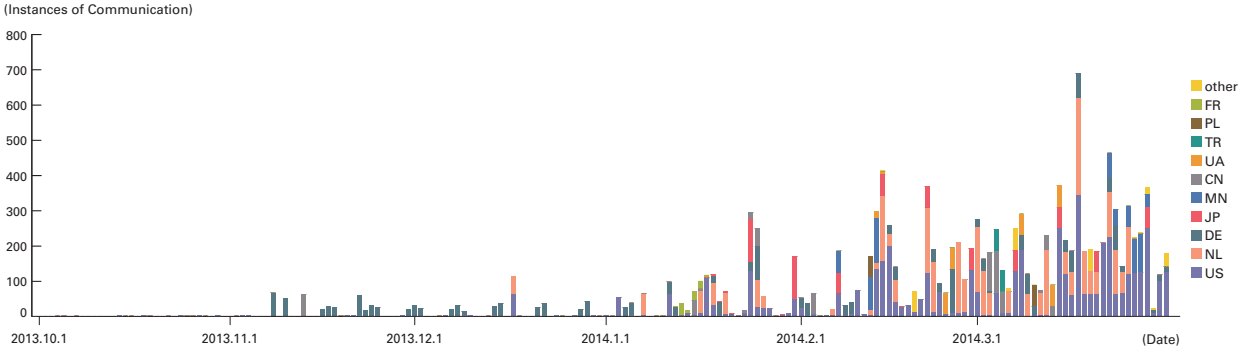


Figure 17: NTP (123/UDP) Traffic Delivered to Honeypots

*73 Version 4.2.7p26 of ntpd and earlier are affected by this vulnerability. See the following ntp.org bug report for more information about the fix. "Bug 1532 - remove ntpd support for ntpdc's monlist (use ntpq's mrulist)" (http://bugs.ntp.org/show_bug.cgi?id=1532).

*74 For example, this applies to FreeBSD. The FreeBSD Project, "ntpd distributed reflection Denial of Service vulnerability" (http://www.freebsd.org/security/advisories/FreeBSD-SA-14:02.ntpd.asc).

*75 CERT/CC, "Vulnerability Note VU#348126 NTP can be abused to amplify denial-of-service attack traffic" (http://www.kb.cert.org/vuls/id/348126).

that much of the traffic originates from Europe and the United States. Japan was the fourth highest source of communications, at 5.9%. From this, we can estimate that verification of the issue and attack attempts increased after the problem was disclosed. Additionally, although queries with the sender misrepresented are sent to exploitable servers in DrDoS attacks, because the total volume of communications observed during this period was not that high, we were unable to determine whether this was scanning behavior for servers or routers that allowed external queries, or attacks targeting the originating host. However, because some sources were IP addresses thought to provide services related to games, we believe that both attacks and scanning behavior were carried out.

■ Dealing with DrDoS Attacks

Because DrDoS attacks are comparatively easy to carry out by spoofing an IP address, when an exploitable vulnerability or new attack method is disclosed, attempts to exploit them tend to be made right away. It is necessary to take note of information about the occurrence of DrDoS attacks, identify whether systems you manage can be exploited in these attacks, and make an effort to deal with any issues.

Additionally, although NTP is identified as the issue in these incidents, protocols such as DNS, SNMP, ECHO, and Chargen could also be exploited in DrDoS attacks. When connecting servers or router devices to the Internet, you must first check vulnerability information for the device, and use a version of firmware, etc., that has no security issues. Furthermore, there are also cases in which services running on devices under default settings are used as stepping stones without users being aware. To avoid this situation, terminate any unnecessary services when installing a device, and configure appropriate access control. After installation, regularly check the running services from the Internet side to detect configuration errors at an early stage, and reduce the likelihood of them being exploited by external third parties.

Because DrDoS attacks involve spoofing the sender, it is possible to limit their impact by implementing suitable communication control. For example, using technology that prevents spoofed communications from flowing into a network, such as source address validation*76, can prevent attacks such as these in which the sender's IP address is spoofed.

A Ministry of Internal Affairs and Communications workshop is also looking into blocking this communication on ISP networks. See "1.4.3 Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business" for more information about this discussion.

■ Summary

As explained here, DrDoS attacks can have a significant impact despite the ease that they can be carried out, so they are a threat that should be taken note of. Meanwhile, although they have been known for a comparatively long time, the fact that there had been few specific threats has meant that sufficient countermeasures have not yet been implemented. We believe that new attacks using similar techniques will appear in the future. To prepare for these, it is essential to properly manage the devices we use on a daily basis. IIJ will continue to play an active role in implementing appropriate measures through industry associations, etc.

1.4.3 Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business*77

Here we discuss the topics covered by the Ministry of Internal Affairs and Communications' "Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business," which was held between November 2013 and March 2014. This workshop is formed from key figures and associations related to telecommunications, and a working group for evaluating technical details is organized under it. Various related associations also assigned their own working groups to evaluate the situation, with many people taking part in a large range of discussions at a number of locations over a short period of time. Only a summary of the topics covered by the workshop are made public, but here we introduce the points discussed based on an initial report that has been made available.

*76 See the following IIJ article for more information about source address validation. "Source Address Validation" (http://www.iij.ad.jp/en/company/development/tech/sav/).

*77 "Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business" (http://www.soumu.go.jp/main_sosiki/kenkyu/denki_cyber/index.html) (in Japanese).

Five Issues Under Scrutiny

This workshop is evaluating the following five issues that relate to recent attacks.

- Blocking access to malware distribution sites*78
- Expanding malware removal based on information obtained from C&C servers
- Preventing new DNSAmp DDoS attacks
- Dealing with spam that exploits SMTP authentication information
- Preventing attacks before they occur, and preventing damages from spreading

Many of these kinds of attacks occur via communications. Communication infrastructure itself may be exposed to attacks, so it is necessary to implement functions for dealing with attacks during the course of communications to a certain degree. Additionally, by dealing with attacks at the ISPs that provide communication services, it is possible to effectively prevent the significant damages that occur. Meanwhile, dealing with attacks over the course of communications involves obtaining information on all communications (including the communication content, and information denoting who carried out communications when and where), using this information to determine whether or not an attack is underway and what its status is, and stopping the attack communications appropriately. This would violate the secrecy of communications as laid out in the Telecommunication Business Act. In other words, it would be unlawful behavior.

In light of this, to deal with attacks in the communications industry it will be necessary to confirm the cause of each attack and its impact, and review the legal justifiability of measures that can be taken. First, it is possible to implement measures to cope with attacks using communications information with the consent of the communicating party concerned, but how to effectively obtain their permission is a large point of contention. Additionally, regardless of whether or not a user has given their permission, implementing measures to cope with attacks could fall under the category of self-defense, averting present danger, or legitimate business operations for providers. These matters are also discussed by this workshop with regard to the five issues. We provide an overview of each of these below*79.

Blocking Access to Malware Distribution Sites

Of the attempts to prevent infection by Web infection malware implemented by the Ministry of Internal Affairs and Communications through their ACTIVE project, the potential for implementing comprehensive URL filtering for all users using a device that intervenes in communications has been evaluated. Conventionally it was deemed that countermeasures using information related to user communications would require individual permission due to the chance that they could be disadvantageous to subscribers in the future. In discussion of this issue, it was decided that blanket permission based on terms and conditions could be considered effective agreement if conditions such as the following were met:

- Users can change their details of consent (can change settings) even after agreeing to the contract clause
- Regardless of changes to the details of consent, other conditions for providing communication services would not change
- It would be implemented by detecting only the necessary minimum amount of communications
- The fact that details of consent can be changed, as well as the method for doing this, would be explained along with an alert screen

Examples of items that should be listed in the contract clause and the alert screen have also been indicated.

*78 This was evaluated as one of the development plans of ACTIVE, a public-private coordination project that conducts proof-of-concept tests for preventing access to malware distribution sites before it occurs, etc. ACTIVE (Advanced Cyber Threats response InitiatiVE), "About ACTIVE" (http://www.active.go.jp/en/active/index.html). Ministry of Internal Affairs and Communications, "Implementing ACTIVE and Holding ACTIVE Promotion Forum" (http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/131001_04.html).

*79 As the case study discussion at this workshop involves legal interpretations with many conditions set, see the workshop's initial report for a more accurate picture of the points discussed.

Expanding Malware Removal Based on Information Obtained From C&C Servers

There are more and more cases in which servers that control malware are seized as a result of the anti-malware activities of a variety of organizations. There was discussion about identifying users that do not know they are infected based on the information stored on these servers, and implementing warnings to convey this fact along with removal methods. In this case, identifying users by searching customer information at ISPs based on source IP addresses and time stamps in information related to communications stored on C&C servers amounts to infringement of the secrecy of communications (external information). During these discussions, there was debate regarding countermeasure methods using records left on C&C servers when the corresponding PCs and devices are actually infected with the malware, and damages are suffered from it. In the end, it was concluded that when information on users identified from their corresponding IP address is only used for the purpose of sending an alert, this constitutes averting present danger, and would be legally justifiable.

Preventing DNSAmp DDoS Attacks

DDoS attacks that generate large volumes of communications using DNS resolvers with insecure configurations as stepping stones (DNSAmp attacks) were observed often in 2013. DNSAmp attacks are made up of several types of communications: those from the attacker to the DNS resolver, those from the DNS resolver to the ISP's DNS server, and amplified responses from Internet-based servers. Here, after debating the status of each type of communication, as well as the effects of implementing measures based on them, we discussed measures for blocking communications from the attacker to the DNS resolver that serves as a stepping stone and prompts amplification. Additionally, because there are a large number of DNS resolvers in the dynamic IP address range that cannot identify a user under normal circumstances, we imagine a situation in which blocks must be implemented comprehensively.

During these discussions, it was decided that with regard to blocking DNS query communications targeting the dynamic IP address space, as long as the results of confirming the target IP address and port number are not used for purposes other than preventing DNSAmp attacks, this constitutes legitimate business operations and is legally justifiable.

Dealing with Spam That Exploits SMTP Authentication Information

SMTP authentication is widely used as a spam countermeasure, but recently due to users reusing the same passwords, etc., it has been targeted in unauthorized access via list-based and other attacks, and in some cases third parties may be exploiting the email transmission function. Here, we discussed two methods for resolving the issue:

- Measures for cases that are highly likely to involve unauthorized use of SMTP authentication IDs and passwords, such as when the connected party shifts to an overseas location instantly. Use is temporarily suspended, and the user is asked to change their password.
- Prevention of attempts to steal IDs and passwords through dictionary attacks, which make many password attempts on specific IDs during the SMTP authentication connection process. When a large number of failed SMTP authentications coming from a specific IP address is detected, SMTP authentication from that IP address is temporarily suspended.

Both cases involve detection based on information related to the status of communication with the server, and temporary suspension of communications. However, as long as this only applies until the unauthorized use is resolved by the user changing their password, or while attacks continue, it was determined that it constitutes legitimate business operations, and is legally justifiable.

Preventing Cyber Attacks Before They Occur and Preventing Damages from Spreading

Discussion of this issue revolved around countermeasures for preventing attacks before they occur by detecting communications including content that exploits system vulnerabilities, and not delivering them to the target destination, as well as countermeasures via coordination between ISPs in simultaneous DDoS attacks or situations in which domestic ISP users are attacking each other. However, because the former involves directly detecting the content of communications, and is an issue that depends on systems with vulnerabilities, and the latter requires preparation work regarding the aspects for which coordination will be necessary before it can be considered, for this initial report it was determined that further discussion would need to be carried out.

As indicated above, this workshop involved discussion of five set issues. For a number of countermeasures in particular, it was concluded that some of them are deemed to have obtained users' consent through blanket permission if it is based on terms and conditions, and that the direct measures against attacks that have been permitted as legitimate self-defense or averting present danger only after the occurrence of attacks were accepted as a legitimate business operation. It can be said that these results will have a significant impact on future consideration of attack countermeasures at ISPs.

Future Activities

The circumstances surrounding Internet-based attacks are changing day-by-day, and even among the specific situations discussed at the workshop, the DDoS attacks that use NTP servers as stepping stones are merely mentioned as an example of those they are aware of occurring. For this reason we believe we should continue this workshop in the future, and evaluate new attacks and their countermeasures.

Additionally, it will be necessary to provide more detailed guidelines for the issues discussed here in situations where they will actually be applied by providers such as ISPs. For example, we need to look into which organizations can be trusted with regard to information when implementing a takedown of C&C servers. Furthermore, regarding anomalies in communications for SMTP authentication, we must attempt to create quantitative standards that make sense to as many users and providers as possible.

For this reason, we will continue to pursue the creation of guidelines for applying the results of this workshop to the practical circumstances of providers, such as at the Council for the Stable Operation of the Internet*80.

1.5 Conclusion

This report has provided a summary of security incidents to which IIJ has responded. In this report, we gave an overview of an investigation into the attackers behind PlugX, and looked into DrDoS attacks and their countermeasures. We also discussed the Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business. 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, IIJSECT 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, and Information Security Operation providers Group Japan.

Hirohide Tsuchiya (1.2 Incident Summary)
Tadaaki Nagao, Hirohide Tsuchiya, Hiroshi Suzuki, Hisao Nashiwa (1.3 Incident Survey)
Hiroshi Suzuki, Takahiro Haruyama (1.4.1 The Attackers Behind PlugX)
Hirohide Tsuchiya (1.4.2 DrDoS Attacks and Countermeasures)
Mamoru Saito (1.4.3 Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business)
Office of Emergency Response and Clearinghouse for Security Information, Service Operation Division, IIJ

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

*80 The Council for the Stable Operation of the Internet is a council formed from communications-related organizations including the Telecommunications Carriers Association, the Telecom Services Association, the Japan Internet Provider's Association, Japan Cable and Telecommunication, and the Telecom Information Sharing and Analysis Center Japan. It draws up the "Guidelines for Dealing with High Volume Communications and Privacy at Telecommunications Carriers." JAIPA, "Revision to Guidelines for Dealing with High Volume Communications and Privacy at Telecommunications Carriers" (http://www.jaipa.or.jp/topics/?p=400) (in Japanese).