Tor Technology

In this report we discuss the Tor system used for anonymous communications, look at the Citadel variant of the ZeuS malware that was used to attack users of Japanese financial institutions in the latter half of last year, and examine a spate of issues affecting protocols and implementations that use cryptographic technology.

1.1 Introduction

This report summarizes incidents to which IIJ responded, based on general information obtained by IIJ itself related to the stable operation of the Internet, information from observations of incidents, information acquired through our services, and information obtained from companies and organizations with which IIJ has cooperative relationships. This volume covers the period of time from October 1 through December 31, 2012. In this period a number of hacktivism-based attacks were once again carried out by Anonymous, and a series of targeted attacks on companies and government-related institutions were discovered. There have also been widespread domain hijackings and alterations on a national scale due to attacks on a number of organizations involved with country-code Top-level Domains (ccTLDs). In Japan, the "Remote Control Virus" and a series of incidents related to it became big news. Malware infections at government-related institutions in Japan are also continuing. 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 October 1 and December 31, 2012. Figure 1 shows the distribution of incidents handled during this period*1.

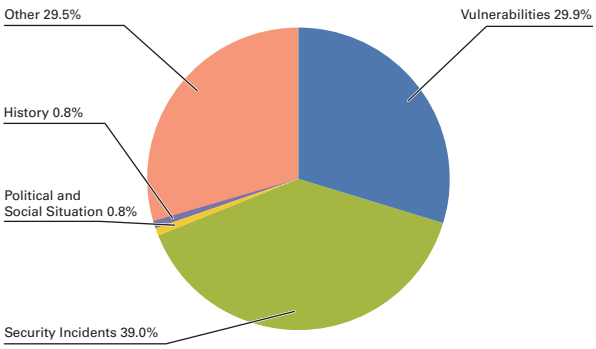

Figure 1: Incident Ratio by Category (October 1 to December 31, 2012)

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. The main activities included attacks on sites related to the Israeli government in protest against aerial bombing and blockades of the Gaza Strip in Palestine carried out by the Israeli army, as well as reprisal attacks on Palestine from Israel (OpIsrael)*2. In Egypt, unrest including violent demonstrations is continuing due to the uproar surrounding a decree published by the president

*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.

*2 For example, the Hackmageddon.com site below provides an overview of attacks made as part of OpIsrael. "Timeline of Opisrael" (http://hackmageddon.com/2012/11/25/timeline-of-opisrael/).

and a referendum on their draft constitution. Attacks were made on sites related to the Egyptian government in support of this movement (OpEgypt). There were also attacks on government agencies in the United Kingdom, Sweden, and Brazil. Other attacks took place around the world on November 5, the British anniversary of Guy Fawkes Day. This day takes its names from Guy Fawkes, who has become the trademark symbol for Anonymous.

In October, the name of a man who bullied a young girl over SNS in Canada and caused her suicide was released (OpRIP). In December, attacks were made on a religious group with extreme views that had announced it would picket the vigils and funerals of victims of a shooting rampage at an elementary school in Connecticut (OpWestBoro). As this demonstrates, Anonymous continues to be very active.

There were also a number of incidents caused by groups other than Anonymous. In October, there were incidents of unauthorized access to servers at universities in Japan and other countries around the world carried out by someone calling themselves TeamGhostShell, and data including stolen account information was published. TeamGhostShell also gained unauthorized access to multiple corporations and government agencies in different countries in December, and leaked approximately 1.6 million account records, etc. they had stolen.

Additionally, the ACTA (Anti-Counterfeiting Trade Agreement) treaty that led to heated protests in European countries was passed at the Japanese Lower House plenary session on September 6, 2012. Following cabinet approval, the instrument of acceptance was deposited on October 5*3. Japan is the first country to ratify the ACTA treaty. However, no attacks of note were observed during this period.

■ Vulnerabilities and their Handling

During this period fixes were released for Microsoft's Windows*4*5*6, Office*7*8, and Internet Explorer*9*10. A large number of vulnerabilities were also discovered and fixed in Adobe Systems' products such as Flash Player and Shockwave Player. Oracle released a scheduled update for Java that fixed many vulnerabilities. Several of these vulnerabilities were exploited in the wild before patches were released.

Regarding server applications, a quarterly update for the Oracle database server was released, fixing a number of vulnerabilities. A vulnerability in BIND DNS servers that caused abnormal server stoppages through the use of certain resource codes was also fixed.

A vulnerability that allowed SQL injections was found and fixed in the popular Web application framework Ruby on Rails, and a hash function vulnerability was also fixed in the Ruby programming language.

■ Attacks on ccTLD

During this period there were a number of attacks on ccTLD and related domain hijacking incidents. First, in October, the IEDR that manages the .ie domain registry for Ireland was accessed without authorization through use of a CMS vulnerability, leading to the hijacking of domains such as Google.ie and Yahoo.ie. In November, servers for the PKNIC that manages the .pk domain registry for Pakistan were hacked by exploiting a SQL injection vulnerability. As a result, 284 domains were hijacked*11. Two

*3 Ministry of Foreign Affairs, "Conclusion of the Anti-Counterfeiting Trade Agreement (ACTA) by Japan" (http://www.mofa.go.jp/policy/economy/i_property/acta_conclusion_1210.html).

*4 "Microsoft Security Bulletin MS12-075 - Critical: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2761226)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-075).

*5 "Microsoft Security Bulletin MS12-078 - Critical: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2783534)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-078).

*6 "Microsoft Security Bulletin MS12-081 - Critical: Vulnerability in Windows File Handling Component Could Allow Remote Code Execution (2758857)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-081).

*7 "Microsoft Security Bulletin MS12-064 - Critical: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2742319)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-064).

*8 "Microsoft Security Bulletin MS12-079 - Critical: Vulnerability in Microsoft Word Could Allow Remote Code Execution (2780642)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-079).

*9 "Microsoft Security Bulletin MS12-071 - Critical: Cumulative Security Update for Internet Explorer (2761451)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-071).

*10 "Microsoft Security Bulletin MS12-077 - Critical: Cumulative Security Update for Internet Explorer (2761465)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-077).

*11 PKNIC (http://www.pknic.net.pk/) made an initial statement regarding this incident. The details can now also be confirmed in other reports.

October 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

O **1st:** Some regulations regarding the incorporation of criminal punishment of illegal downloading came into effect due to the amended Copyright Act.
Agency for Cultural Affairs, "2012 Regular Diet Session - Regarding Copyright Act Amendments"
(http://www.bunka.go.jp/chosakuken/24_houkaisei.html) (in Japanese).

S **2nd:** TeamGhostShell accessed servers at a number of universities around the world without authorization, and published stolen information. Several Japanese universities were also affected by this incident.
For example, the following statement from the University of Tokyo that multiple Web servers there were accessed without authorization, and information such as IDs and email addresses were leaked. The University of Tokyo "Regarding Information Leaks Due to Unauthorized Access at Our University" (http://www.u-tokyo.ac.jp/public/public01_241005_02_j.html) (in Japanese).

O **4th:** ENISA hosted a large-scale cyber attack exercise, "Cyber Europe 2012," in which approximately 300 companies participated.
ENISA, "Europe joins forces in Cyber Europe 2012"
(http://www.enisa.europa.eu/media/press-releases/europe-joins-forces-in-cyber-europe-2012).

S **7th:** Reports revealed that the wrong people had been arrested in multiple incidents in which abusive messages were posted to websites using the "Remote Control Virus".

V **9th:** 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://www.adobe.com/support/security/bulletins/apsb12-22.html).

V **9th:** Microsoft re-released update programs because some of the digital certificates used to sign binaries did not contain proper timestamp attributes, adversely affecting the ability to install or uninstall security update programs, etc.
"Microsoft Security Advisory (2749655) Compatibility Issues Affecting Signed Microsoft Binaries"
(http://technet.microsoft.com/en-us/security/advisory/2749655).

S **9th:** The IEDR domain registry for Ireland was accessed without authorization, leading to the hijacking of Google.ie and Yahoo.ie.
See the following IEDR statement for more information. "IEDR Security Statement"
(https://www.iedr.ie/wp-content/uploads/2012/12/IEDR-Statement-D-issued-8Nov.pdf).

V **10th:** Microsoft began automatic updates for the Windows update program restricting use of certificates using RSA keys less than 1024 bits in length that was published in August.
"Microsoft Security Advisory (2661254) Update For Minimum Certificate Key Length"
(http://technet.microsoft.com/en-us/security/advisory/2661254).

V **10th:** Microsoft published their Security Bulletin Summary for October 2012, and released the MS12-064 critical update as well as six important ones.
"Microsoft Security Bulletin Summary for October 2012" (http://technet.microsoft.com/en-us/security/bulletin/ms12-oct).

V **10th:** A vulnerability (CVE-2012-5166) in BIND 9.x that could allow external parties to cause a crash using specially crafted data was discovered and fixed.
Internet Systems Consortium, "CVE-2012-5166: Specially crafted DNS data can cause a lockup in named" (https://kb.isc.org/article/AA-00801/0).

O **10th:** The "Fifth Japan-ASEAN Information Security Policy Meeting" aimed at bolstering international cooperation and initiatives with ASEAN countries was held in Japan.
National Information Security Center, "Outcome of the Fifth Japan-ASEAN Information Security Policy Meeting"
(http://www.nisc.go.jp/press/pdf/5th_aseanj_meeting_result_press.pdf) (in Japanese).

V **11th:** A vulnerability that could allow remote third parties to gain control by bypassing authentication was discovered in the Web management screen of network cameras from a number of vendors.
US-CERT "Multi-vendor IP camera web interface authentication bypass" (http://www.kb.cert.org/vuls/id/265532).

V **17th:** Oracle released their quarterly scheduled update for Java SE JDK and JRE, fixing 30 vulnerabilities including those that allowed execution of arbitrary code.
"Oracle Java SE Critical Patch Update Advisory - October 2012" (http://www.oracle.com/technetwork/topics/security/javacpuoct2012-1515924.html).

O **23rd:** A number of inappropriate items in the terms of use and device access permissions for a free call app for smartphones became an issue when discovered, as they could be interpreted to allow information to be provided to third parties, and they also requested excessive permissions.

V **24th:** A number of vulnerabilities in Adobe Shockwave Player that could allow arbitrary code execution were discovered and fixed.
"Security update available for Adobe Shockwave Player" (http://www.adobe.com/support/security/bulletins/apsb12-23.html).

O **25th:** Microsoft released their new Windows 8 OS, which includes an improved user interface and security functions.

O **27th:** The "Hardening One" security event where the overall operational capabilities of IT systems are contested was held.
See the following WASForum post regarding the Hardening Project for more information (http://wasforum.jp/hardening-project/) (in Japanese).

O **30th:** The "anti-Malware engineering WorkShop 2012 (MWS2012)" for presenting the results of research on malware countermeasures and cultivating human resources for anti-malware activities was held.
"anti-Malware engineering WorkShop 2012 (MWS2012)" (http://www.iwsec.org/mws/2012/index.html) (in Japanese).

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

*Dates are in Japan Standard Time

days later, it was reported that similar incidents had occurred at Romanian domains (.ro). In December, there were more domain hijackings after the registrar for Serbian .rs domains was attacked. In each of these incidents, well-known domains for global corporations such as Google, Yahoo!, and PayPal were targeted, and users were redirected to fraudulent sites.

When an attack on a registry or registrar that manages ccTLD succeeds, it is possible to hijack many domains all at once, including those accessed by a large number of people. Additionally, as shown in cases reported on the Kaspersky Lab blog*12, because fake IP addresses are returned even when querying an external DNS server thought to be trustworthy such as Google Public DNS, the average user is not likely to notice. As this illustrates, we believe attempts to make similar attacks on organizations that manage ccTLD will continue, because this can affect a large number of users without them being aware of it.

■ Smartphone Applications and Service Integration

A vulnerability in the Skype communication app's web-based password reset function was discovered and fixed*13. The spread of a worm that propagates through Skype instant messages has also been reported*14. An issue occurred with the LINE communication app, causing LINE friends to be automatically added from contact information when the "Off" setting for a function that automatically adds friends failed to work correctly after an update to the Android version of the application*15. There were also issues with its Facebook integration function, which would not sync correctly when the friend integration function for Facebook accounts was used*16.

Individual apps on smartphones can offer more convenience through integration with external SNS, so this kind of integration is on the rise. On the other hand, however, integration apps with malicious intent have also been identified, including those that perform actions or post comments without the user's intention, or collect personal information from a device. IPA released a statement about incidents of this kind in which posts are made on SNS without the user's knowledge due to exploitation of app service integration functions. It contained specific examples of this, and summarized countermeasures such as cancelling unnecessary integration services*17.

■ Government Agency Initiatives

A number of attacks on government agencies once again become a topic of discussion during this period. In October, an incident occurred in which emails misrepresented as being from the Cabinet Office were distributed, echoing a similar incident in April*18. Additionally, it was announced that the computer of an employee at the Japan Aerospace Exploration Agency (JAXA) had been infected by a computer virus, and rocket-related information had possibly been leaked externally*19. Similarly, an incident in which a computer used by an employee of the Japan Atomic Energy Agency was infected by a computer virus also occurred*20.

Government agency activities included the 8th assembly of the Council for Promotion of Information Security Measures, which promotes security measures for government agencies. At this assembly revisions were made to define specific dates for transition guidelines covering cryptographic algorithms at government agencies. These are being worked on due to the compromise of SHA-1 and RSA1024. Reports were also made on cyber attacks against government agencies that took place in September, and on the status of initiatives for information security measures at government agencies*21.

---

*12 See the following Kaspersky Lab SECURELIST Blog post for more details. "Google.ro and other RO domains, victims of a possible DNS hijacking attack" (http://www.securelist.com/en/blog/208194028Google_ro_and_other_RO_domains_victims_of_a_possible_DNS_hijacking_attack).

*13 Kaspersky Lab SECURELIST Blog, "New Skype vulnerability allows hijacking of your account" (http://www.securelist.com/en/blog/208193933/New_Skype_vulnerability_allows_hijacking_of_your_account).

*14 Trend Micro, "Trend Micro - Monthly Report on Virus Infections [Oct. 2012]" (http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20121105073724.html) (in Japanese).

*15 NAVER LINE, "An Apology and News of a Fix for a Bug in the Android Version of LINE 3.3.0" (http://lineblog.naver.jp/archives/20587620.html) (in Japanese).

*16 NAVER LINE, "We've stopped the integration function for Facebook friends on the Android version of LINE." (http://en.lineblog.naver.jp/archives/20505343.html).

*17 IPA, "October 2012 Address 'Beware Service Integration on SNS!' - Your Name Can Be Used Without Your Knowledge - " (http://www.ipa.go.jp/security/txt/2012/10outline.html) (in Japanese).

*18 Cabinet Office, "Regarding Emails Misrepresented as being from the Cabinet Office" (http://www.cao.go.jp/press/20121011notice.html) (in Japanese).

*19 Japan Aerospace Exploration Agency (JAXA), "Regarding a Computer Virus Infection at JAXA and Potential Information Leaks" (http://www.jaxa.jp/press/2012/11/20121130_security_j.html) (in Japanese).

*20 Japan Atomic Energy Agency, "Concerning Potential Information Leaks due to a Computer Virus Infection" (http://www.jaea.go.jp/02/press2012/p12120501/index.html) (in Japanese). It was later announced that email addresses may have been leaked. "Concerning Potential Personal Information Leaks due to a Computer Virus Infection" (http://www.jaea.go.jp/02/press2012/p13011801/index.html) (in Japanese).

*21 National Information Security Center, "8th Assembly of the Council for Promotion of Information Security Measures (Liaison Conference for CISO, etc.) (Oct. 26, 2012)" (http://www.nisc.go.jp/conference/suishin/index.html#2012_5) (in Japanese).

November Incidents

1 **1st:** The "Convention on Cybercrime" ratified in July 2011 came into effect.
Ministry of Foreign Affairs, "Convention on Cybercrime" (http://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html) (in Japanese).

2 **2nd:** The Ministry of Internal Affairs and Communications published "Tips for General Users to Use Wireless LAN Safely," which describes the bare minimum measures that users should take to use wireless LAN with peace of mind.
3 "Publication of 'Tips for General Users to Use Wireless LAN Safely'" (http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000029.html) (in Japanese).

4 **6th:** A BGP routing anomaly occurred at an Indonesian ISP due to a hardware fault, affecting Google's GoogleApps among others.
5 More detailed information has been reported on the following CloudFlare Blog. "Why Google Went Offline Today and a Bit about How the Internet Works" (http://blog.cloudflare.com/why-google-went-offline-today-and-a-bit-about).

6 **6th:** Financial institutions and other organizations issued an alert after the discovery of new fraud techniques for posing as a financial institution. These involve displaying a fraudulent pop-up message that prompts users to enter details after they log in to a legitimate site.
7 For example, the National Police Agency issued the following alert. "Regarding Measures for Cases of New Techniques Targeting the Personal Information of Internet Banking Users, etc." (www.npa.go.jp/cyber/warning/h24/121106.pdf) (in Japanese)

8 **7th:** 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://www.adobe.com/support/security/bulletins/apsb12-24.html).

9 **7th:** The United States presidential election was held.

10 **8th:** A vulnerability in Adobe Reader X/XI with no fix available that circumvents the sandbox protection function to execute arbitrary code was disclosed.
11 The following Group-IB announcement contains more information, but Adobe states that no fix can be made because detailed information has not been provided, and they cannot confirm the vulnerability. "Group-IB US: Zero-day vulnerability found in Adobe X" (http://www.group-ib.com/index.php/7-novosti/672-group-ib-us-zero-day-vulnerability-found-in-adobe-x).

12 **9th:** Emails stating that user passwords had been reset due to the possibility that accounts had been hacked were sent by mistake to many Twitter users, caused confusion for them.
13 Twitter, "Password reset emails" (http://status.twitter.com/post/35275426563/password-reset-emails).

14 **10th:** A vulnerability (CVE-2012-5371) in Ruby 1.9 that could cause crashes through hashing-flooding attacks was discovered and fixed
Ruby Community, "Hash-flooding DoS vulnerability for ruby 1.9 (CVE-2012-5371)"
15 (http://www.ruby-lang.org/en/news/2012/11/09/ruby19-hashdos-cve-2012-5371/).

16 **14th:** Microsoft published their November 2012 security bulletin, and released four critical updates including MS12-071 and MS12-075, as well as one important update and one warning update.
"Microsoft Security Bulletin Summary for November 2012" (http://technet.microsoft.com/en-us/security/bulletin/ms12-nov).

17 **15th:** A bug in a number of Android devices that caused crashes through accessing an improper memory region when specific system files are accessed if the Linux kernel settings were incorrect was discovered and fixed.
18 JVN, "JVN#74829345 Multiple Android devices vulnerable to denial-of-service (DoS)" (http://jvn.jp/en/jp/JVN74829345/).

19 **18th:** It was announced that unauthorized access had taken place at FreeBSD.org since September. This is thought to have been caused by the leak of a developer's SSH key.
The FreeBSD Project., "Security Incident on FreeBSD Infrastructure" (http://www.freebsd.org/news/2012-compromise.html).

20 **19th:** JNSA published a report called "Safely Navigating SNS," which summarizes problems related to SNS security and privacy.
21 "Safely Navigating SNS - Security and Privacy Issues and Countermeasures" (http://www.jnsa.org/result/2012/SNS-WG_ver0.7.pdf) (in Japanese).

22 **20th:** A fault occurred on NTP servers at the United States Naval Observatory, causing system trouble due to the wrong times being reported.
23 See the following Microsoft blog post for more information. "Fixing When Your Domain Traveled Back In Time, the Great System Time Rollback to the Year 2000" (http://blogs.technet.com/b/askpfeplat/archive/2012/11/26/fixing-when-your-domain-traveled-back-in-time-the-great-system-time-rollback-to-the-year-2000.aspx).

24 **20th:** The Japan Data Communications Association published an "Important Notice Regarding the Use of Provider Services such as Data Centers [Alert]" in response to data loss issues at hosting service providers.
25 "Important Notice Regarding the Use of Provider Services such as Data Centers [Alert]" (http://www.dekyo.or.jp/pmark/sinsei/data/tyuikanki.pdf) (in Japanese).

26 **26th:** An employee of an outsourcing contractor working on the development of a system for a financial institution was arrested for forging a cash card and using it to withdraw money.

27 **27th:** A vulnerability was discovered in multiple Samsung printers, which contained a hardcoded SNMP community string that caused administrative functions to be enabled even when disabled in settings.
28 US-CERT, "Vulnerability Note VU#281284 Samsung Printer firmware contains a hardcoded SNMP community string" (http://www.kb.cert.org/vuls/id/281284).

29 **28th:** The registry for Romania's .ro domains was accessed without authorization, and multiple domains including well-known examples such as Google and Yahoo! were hijacked.

30 **30th:** The Japan Aerospace Exploration Agency (JAXA) announced that an employee's computer had been infected with a computer virus, and as a result rocket-related information may have leaked.
"Regarding a Computer Virus Infection at JAXA and Potential Information Leaks" (http://www.jaxa.jp/press/2012/11/20121130_security_j.html) (in Japanese).

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

*Dates are in Japan Standard Time

Initiatives for international collaboration continue, and the Fifth Japan-ASEAN Information Security Policy Meeting was held in Japan in October. It promoted initiatives such as raising awareness of information security, evaluating systems for sharing data related to information security, checking points of contact, and further enhancing collaborations on information security.

■ Threats and Measures for Control Systems

In addition to use in production equipment at factories, control systems play an increasing role as infrastructure systems for equipment that requires a high level of management. This includes key services in our lives and social activities such as water supply system management, the energy field such as electricity and gas, and atomic energy facilities.

Meanwhile, as the use of control systems that integrate telecommunications technology progresses, the discovery of vulnerabilities in devices and software related to control systems has become a problem. A number of issues caused by attacks and malware infections targeting control systems have also been identified*22.

A newsletter regularly published by the U.S. ICS-CERT CSIRT organization that specializes in control systems also confirmed that threats to control systems are on the rise. Under these circumstances, the need for security management of control systems in Japan is increasing. In response, IPA published "A practical guide to IEC62443-2-1 (CSMS: Cyber Security Management System), which specifies requirements related to security management for control systems when constructing them"*23.

■ The "Remote Control Virus"

During this period, a series of incidents related to the "Remote Control Virus" attracted attention. From around June 2012, a large number of death threats and bomb threats were made via email and message boards. These incidents involved threats and warnings targeting government agencies and local authorities, multiple companies and events, as well as individuals. In a number of cases, this led to responses such as the tightening of security or cancellation of events, including the cancellation of a flight in progress due to a bomb scare. However, in October it came to light that these crimes may have been committed by a third party using the arrested suspects' PCs, which were infected with a virus. Furthermore, emails claiming responsibility were sent to law firms and news outlets such as radio stations by someone claiming to be the true culprit, raising the possibility that a number of the threatening comments and postings might have been made by this person.

These incidents have two major characteristics. Firstly, it is believed that the Tor tool for anonymizing communication routes such as message board postings and emails sent was used to make it harder to identify the user. See "1.4.1 An Overview of Tor" for more information about Tor.

Secondly, multiple attack methods were used for these crimes. One was cross-site request forgery (CSRF), in which an URL that posted criminal threats to a posting form on the website of a local public body was posted to a large message board in Japan, causing message board users who clicked this link to unintentionally post threats to the corresponding organization. Another method was remote control via a self-authored virus, in which a virus is installed on the PC of a third party under the guise of a freeware application, and criminal threats posted to a message board from that PC via remote control using commands written on another message board*24.

*22 For example, the Stuxnet malware that targeted industrial control systems, which was discovered in 2010.

*23 ICS-CERT, "ICS-CERT Newsletter the 'ICS-CERT Monthly Monitor,' October-December 2012" (http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf). IPA released a summary in Japanese "ICS-CERT Monthly Monitor (October-December 2012) Overview" (http://www.ipa.go.jp/security/controlsystem/pdf/MonthlyReport_201210-12_r3.pdf) (in Japanese).
IPA, "Publication of a practical guide for building security management systems for control systems" (http://www.ipa.go.jp/security/fy24/reports/ics_management/index.html) (in Japanese).

*24 Details of this series of incidents and appeals for information appeared on the Metropolitan Police Department website and Facebook page until the suspect was arrested in February 2013.

December Incidents

1 2 3

O **3rd:** The ITU World Conference on International Telecommunications (WCIT-12) was held in Dubai, United Arab Emirates. A number of proposals for revision became a topic of conversation there, including the tightening of Internet regulations, with revisions to the International Telecommunication Regulations (ITR).
An amended version of the ITR was adopted at the conference, but Japan did not sign it. See the following Ministry of Internal Affairs and Communications report for more information on discussions at the conference. Ministry of Internal Affairs and Communications, "ITU World Conference on International Telecommunications (WCIT-12)" (http://www.soumu.go.jp/menu_seisaku/ictseisaku/cyberspace_rule/wcit-12.html) (in Japanese).

4 5 6

V **5th:** A vulnerability (CVE-2012-5688) in BIND 9.x that could allow external parties to cause a crash using specially crafted data was discovered and fixed.
Internet Systems Consortium, "CVE-2012-5688: BIND 9 servers using DNS64 can be crashed by a crafted query" (https://kb.isc.org/article/AA-00828).

S **5th:** The Council of Anti-Phishing Japan published their "Consumer-Oriented Guidelines for Preventing Phishing Fraud," which gives examples of the damages caused by phishing fraud, and indicates how it can be prevented.
Council of Anti-Phishing Japan, "Consumer-Oriented Guidelines for Preventing Phishing Fraud" (http://www.antiphishing.jp/report/pdf/consumer_antiphishing_guideline.pdf) (in Japanese).

7 8

S **5th:** The registrar for Serbia's .rs domains was accessed without authorization, and multiple domains including well-known examples such as Google and Yahoo! were hijacked.
See the following RNIDS report for more information. "The official statement from NiNet Company given on 05 December" (http://www.rnids.rs/en/what-s-new/%D1%82he-official-statement-from-ninet-company-given-on-05-december/id/4035).

9 10

S **10th:** TeamGhostShell accessed a number of aerospace-related companies around the world without authorization, and released 1.6 million pieces of stolen account information, etc. (#ProjectWhiteFox).

11

S **11th:** It was reported that targeted attacks had been made on multiple Russian companies from Korea.
Details can be found in the following Fireeye blog post. "To Russia With Targeted Attack" (http://blog.fireeye.com/research/2012/12/to-russia-with-apt.html).

12 13

O **11th:** The National Information Security Center held the "CIIREX 2012" interdisciplinary exercise for critical infrastructure.
NISC, "Summary of Interdisciplinary Exercise for Critical Infrastructure [CIIREX 2012]" (http://www.nisc.go.jp/active/infra/pdf/ciirex2012_2_press.pdf) (in Japanese).

14

V **12th:** Microsoft published their Security Bulletin Summary for December 2012, and released five critical updates including MS12-077 and MS12-079, as well as two important updates.
"Microsoft Security Bulletin Summary for December 2012" (http://technet.microsoft.com/en-us/security/bulletin/ms12-dec).

15 16

V **12th:** A vulnerability in Microsoft Internet Explorer versions 6 to 10 that allowed the position of the mouse cursor on the screen to be detected using JavaScript on any website was disclosed.
See the following blog post from UK-based spider.io who discovered the vulnerability for more information. "Internet Explorer Data Leakage" (http://spider.io/blog/2012/12/internet-explorer-data-leakage/).

17 18

V **12th:** A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"APSB12-27: Security updates available for Adobe Flash Player" (http://www.adobe.com/support/security/bulletins/apsb12-27.html).

動 **12th:** North Korea launched a satellite as they had previously announced.

19 20

S **14th:** A junior high school student was referred to prosecutors on suspicion of violating the Act on the Prohibition of Unauthorized Computer Access by obtaining free email passwords without authorization and spying on email. In this incident, a feature for users who had forgotten their password was exploited to obtain passwords.

21

O **16th:** The 46th Lower House general election was held.

22 23

V **17th:** A vulnerability that could allow root privileges to be obtained was reported in devices containing the South Korean Samsung's Exynos mobile phone CPU.
XDA Developers, "Dangerous Exynos 4 Security Hole Demoed and Plugged by Chainfire" (http://www.xda-developers.com/android/dangerous-exynos-4-security-hole-demoed-and-plugged-by-chainfire/).

24 25

O **20th:** IPA published their "2011 Survey on Damages Related to Information Security Events" report, which summarizes trends and countermeasures for information security damages. It points out the impact of damages caused by the fraudulent activity of insiders, and the fact that measures for protecting data on devices such as smartphones are currently insufficient.
"Publication of the '2011 Survey on Damages Related to Information Security Events'" (http://www.ipa.go.jp/about/press/20121220.html) (in Japanese).

26 27

V **21st:** Microsoft re-released a problematic update (MS12-078) related to a number of Windows vulnerabilities, including those that could allow arbitrary code execution through viewing a malicious website that were disclosed on the 12th.
"Microsoft Security Bulletin MS12-078 - Critical: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2783534)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-078).

28 29

V **22nd:** A vulnerability (CVE-2012-6496) in Ruby on Rails methods that could allow remote SQL injection attacks was discovered and fixed. This vulnerability was initially assigned to CVE-2012-5664, but was later split into CVE-2012-6496 and CVE-2012-6497.
JVN, "JVNDB-2013-001006 An SQL injection vulnerability in the Authlogic gem for Ruby on Rails" (http://jvndb.jvn.jp/ja/contents/2013/JVNDB-2013-001006.html) (in Japanese).

30 31

V **31st:** A vulnerability in Microsoft's Internet Explorer that could allow arbitrary code execution through viewing a malicious website was disclosed.
"Microsoft Security Advisory (2794220) Vulnerability in Internet Explorer Could Allow Remote Code Execution" (https://technet.microsoft.com/en-us/security/advisory/2794220). This issue was fixed with "Microsoft Security Bulletin MS13-008 - Critical: Security Update for Internet Explorer (2799329)" (http://technet.microsoft.com/en-us/security/bulletin/ms13-008) in January.

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

*Dates are in Japan Standard Time

Neither of these methods are new, as they have been used often in the past. Regarding CSRF, there was a furor in 2005 over the unintentional posting of the diary entries of users who clicked an URL on a SNS site, for example. Examples of remote control viruses include Back Orifice*25, which attracted interest as far back as 1998, and attacks made by the malware known as Shady RAT that attracted interest last year, which has a remote control function*26.

Some of those accused in these incidents fell victim to identity theft after a virus was installed when they tried to install a freeware application mentioned on message boards. Care must be taken to avoid falling prey to this kind of crime, by not downloading or using files of unknown origin without taking precautions, even when they supposedly have useful functions, and by using caution when accessing links. Another basic measure that must be taken is always keeping your OS, applications, and anti-virus software definition files up to date.

■ Other

In November, Syria made news when its Internet and mobile phone connections were almost completely shut down*27. The cause was initially announced to be the severing of cables by terrorists, but two days later connections were re-established, and it was explained that a fault at a power transmission facility had caused the issue. Syria also faced Internet blackouts in June, and some have suggested that this may have been government regulation of information*28.

Regarding Internet regulations, the first revisions to the International Telecommunication Regulations (ITR) in 24 years at the ITU World Conference on International Telecommunications (WCIT-12) held in Dubai in December attracted attention. The ITR was amended at the conference, but Japan, the United States, and European Union Nations were among 55 countries that put off signing, because the draft revisions and resolutions adopted could lead to a tightening of regulations for Internet content, as well as censorship.

In Germany, a power grid operator made news when it was the target of a DDoS attack*29. This was an attack on Internet-based communication systems such as Web servers and email, rather than an attack on the power grid itself, but with smart meters and smart grid*30 technology becoming more prevalent, it has been said that attacks on network-connected power grids may increase in the future.

In the United States, a perpetrator arrested on suspicion of nine felonious crimes including unauthorized access in October 2011, relating to the theft and leaking of private information such as the email accounts of Hollywood actresses and celebrities, was sentenced to 10 years in prison*31.

Phishing incidents utilizing email and SNS also continue to occur. Furthermore, in incidents relating to financial institutions, a new technique had been identified in which a fraudulent pop-up message that prompts users to enter details is displayed after the user logs in to a legitimate site. These are attempts to infect the user's PC with malware, and steal their secondary authentication information such as passwords and random number tables when they are using Internet banking. Alerts were issued after attacks based on similar techniques were confirmed at a number of fin ancial institutions. Supposedly, multiple malware such as variants of SpyEye and ZeuS were used in these attacks. See "1.4.2 The Citadel Variant of ZeuS" for more information on ZeuS variants.

*25 Back Orifice is called remote control software, but because it has a mode in which it hides itself to conceal the fact that it is running, and functions that allow it to be installed without users noticing, it is classified as malware by anti-virus software vendors.

*26 See McAfee's "Revealed: Operation Shady RAT" (http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf) for more information.

*27 CloudFlare Blog, "How Syria Turned Off the Internet" (http://blog.cloudflare.com/how-syria-turned-off-the-internet).

*28 Renesys Blog, "Syrian Internet Shutdown" (http://www.renesys.com/blog/2011/06/syrian-internet-shutdown.shtml).

*29 The National Electric Sector Cybersecurity Organization (NESCO), "News reports of attack on 50Hertz" (http://www.us-nesco.org/tac-diary/news-reports-of-attack-on-50hertz/).

*30 Power grids that prevent blackouts and adjust power transmission efficiently utilizing power meters featuring communication/control functions as well as smart meters.

*31 FBI, "Florida Man Convicted in Wiretapping Scheme Targeting Celebrities Sentenced to 10 Years in Federal Prison for Stealing Personal Data" (http://www.fbi.gov/losangeles/press-releases/2012/florida-man-convicted-in-wiretapping-scheme-targeting-celebrities-sentenced-to-10-years-in-federal-prison-for-stealing-personal-data).

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 Defense Service between October 1 and December 31, 2012. This information shows traffic anomalies judged to be attacks based on IIJ DDoS Defense Service standards. IIJ also responds to other DDoS attacks, but these incidents are excluded from the figure due to the difficulty in accurately ascertaining the facts of each situation. There are many methods that can be used to carry out a DDoS attack, and the capacity of the environment attacked (bandwidth and server performance) will largely determine the degree of impact. Figure 2 categorizes DDoS attacks into three types: attacks on bandwidth capacity*32, attacks on servers*33, 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 901 DDoS attacks. This averages to 9.79 attacks per day, indicating an increase in the average daily number of attacks compared to our prior report. Bandwidth capacity attacks accounted for 0.3% of all incidents, server attacks accounted for 79.7%, and compound attacks accounted for the remaining 20.0%.

The largest attack observed during the period under study was classified as a compound attack, and resulted in 212Mbps of bandwidth using up to 38,000pps packets.

Of all attacks, 84.5% ended within 30 minutes of commencement, 14.5% lasted between 30 minutes and 24 hours, and 1.0% lasted over 24 hours. The longest sustained attack was a server attack that lasted for one day, four hours, and 10 minutes (28 hours and 10 minutes).

In most cases, we observed an extremely large number of IP addresses, whether domestic or foreign. We believe this is accounted for by the use of IP spoofing*34 and botnet*35 usage as the method for conducting DDoS attacks.

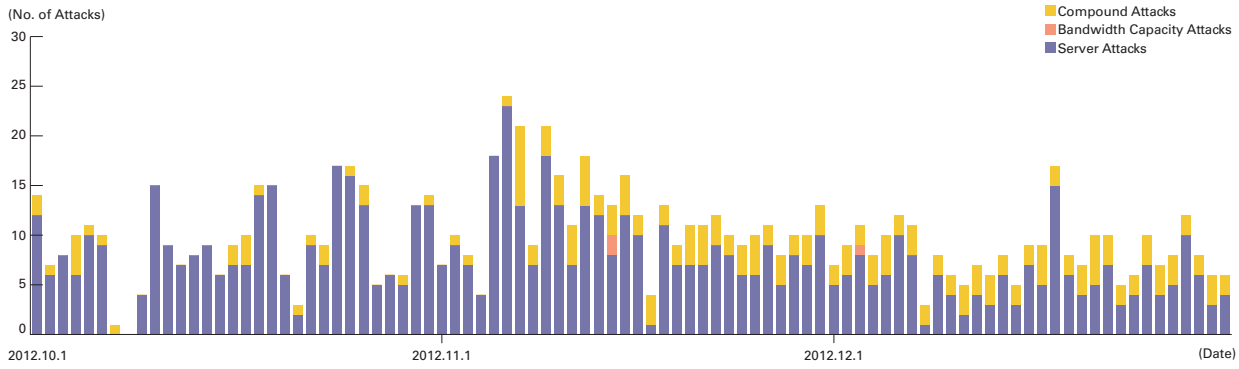

Figure 2: Trends in DDoS Attacks

*32 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.

*33 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.

*34 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.

*35 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*36 set up by the MITF, a malware activity observation project operated by IIJ*37. By monitoring backscatter it is possible to detect some of the DDoS attacks occurring on external networks as a third party without any interposition.

For the backscatter observed between October 1 and December 31, 2012, 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 44.8% of the total during the target period. Attacks on ports such as 443/TCP used for HTTPS, 5100/TCP used for video chat, etc., and 22/TCP used for SSH were also observed. Looking at the origin of backscatter thought to indicate IP addresses targeted by DDoS attacks by country in Figure 3, the United States and Singapore accounted for large proportions at 37.3% and 19.5%, respectively, with other countries following in order.

Regarding particularly large numbers of backscatter packets observed, there were attacks on the Web servers (80/TCP) for a domain registrar and a search-related service provider in the United States between November 23 and November 24. On November 19, backscatter was observed from multiple Web servers, indicating attacks on Web servers in the Netherlands, and those for a game-related provider in the United States, a server provider in the United States, and an adult site in Turkey. On December 21, backscatter from a Lebanese financial institution and a United States religious organization was observed. On this day, attacks on the Web servers for a number of hosting providers in the United States and Russia were also observed.

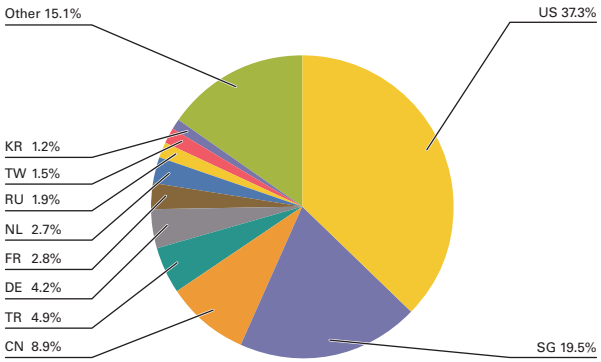

Figure 3: Distribution of DDoS Attack Targets According to Backscatter Observations (by Country, Entire Period under Study)

Many attacks on Web servers (443/TCP) were observed between October 30 and November 8. These were linked to attacks on a number of Web servers for a hosting provider in Singapore. In these attacks backscatter was observed over 10,000 times from some servers, and it is thought that the attack was quite sizable. Between November 12 and November 15, a total of over 10,000 5100/TCP attacks were observed on servers in China. On December 19, a large number of 5114/TCP attacks were also observed on servers in China. These ports are not normally used by standard applications, so the purpose of the attacks is not known.

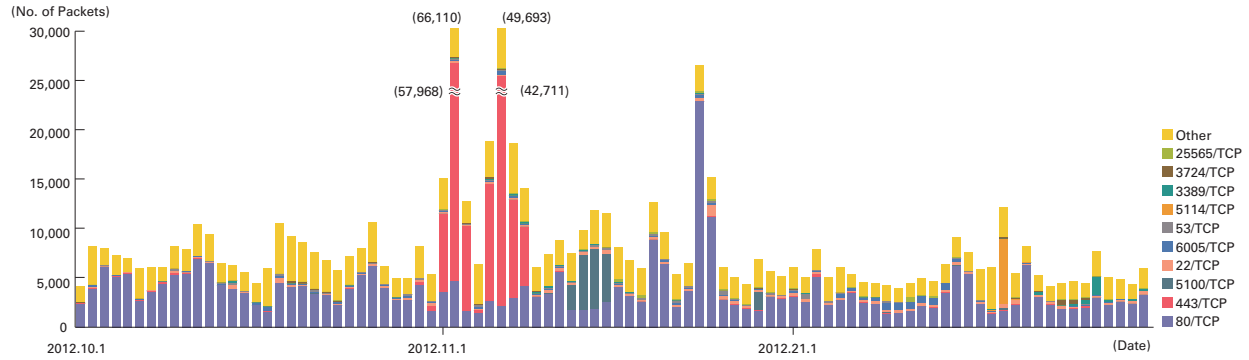

Figure 4: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)

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

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

Notable DDoS attacks during the current survey period that were detected via IIJ's observations of backscatter included attacks on multiple Swedish government agencies in October thought to have been made by Anonymous. Also in October, attacks thought to be the work of The Wiki Boat Brazil were detected on Brazil's Ministry of Finance and Federal Police. In November, there were attacks on a number of torrent sites thought to be carried out by AnonymousZeiko, and attacks on Interpol considered to be the work of the Kosovo Hacker. In December, Anonymous is believed to have been behind attacks on a religious group that exhibits radical behavior.

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 October 1 and December 31, 2012. 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.

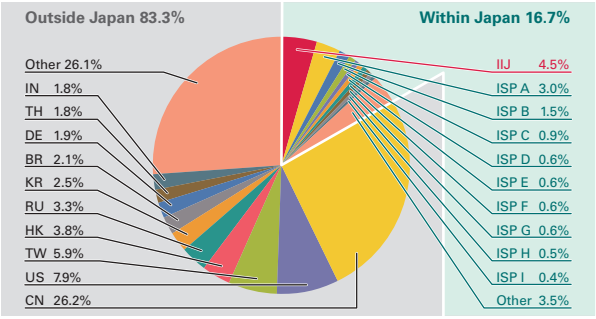

Figure 5: Sender Distribution (by Country, Entire Period under Study)

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, 23/TCP used for telnet, and ICMP echo requests. Additionally, communications of an unknown purpose were observed on ports not used by common applications, such as 38327/UDP.

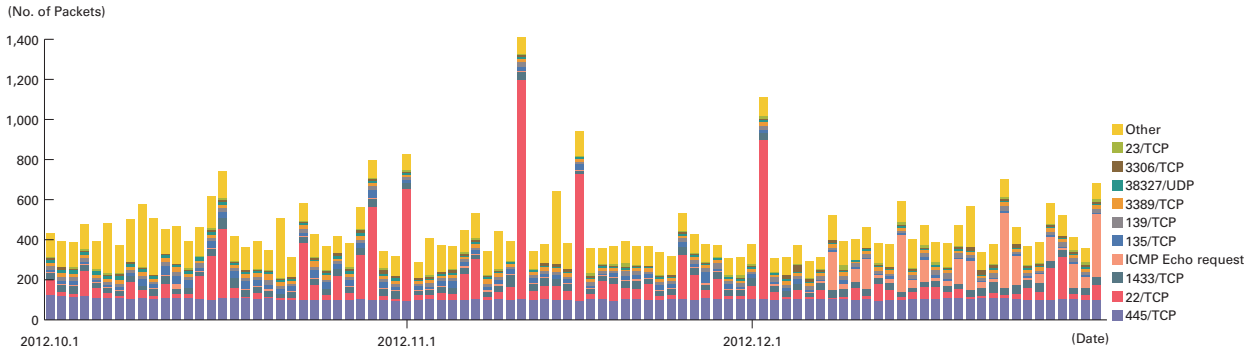

Figure 6: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

*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.

Communications thought to be SSH dictionary attacks also occurred during the current period. For example, concentrated communications were observed coming from individual IP addresses in Germany on October 29, China on November 1, Thailand and Turkey on November 11, China on November 16, and Singapore on December 2. ICMP echo requests also increased intermittently after December 8. This mainly involved communications from two IP addresses to a specific honeypot, but action was not taken because no actual harm was done.

■ Malware Network Activity

Figure 7 shows the distribution of the specimen acquisition source for malware during the period under study, while Figure 8 shows trends in the total number of malware specimens acquired. Figure 9 shows trends in the number of unique specimens. In Figure 8 and Figure 9, the number of acquired specimens show the total number of specimens acquired per day*40, while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*41.

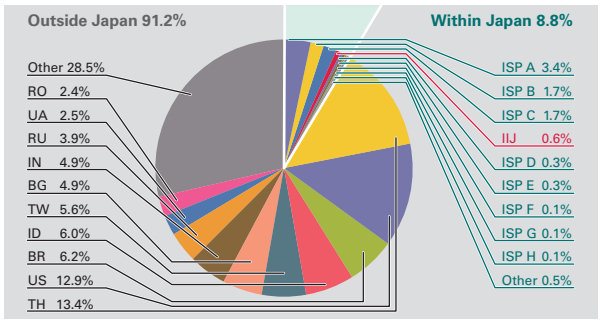

Figure 7: Distribution of the Number of Malware Specimens Acquired

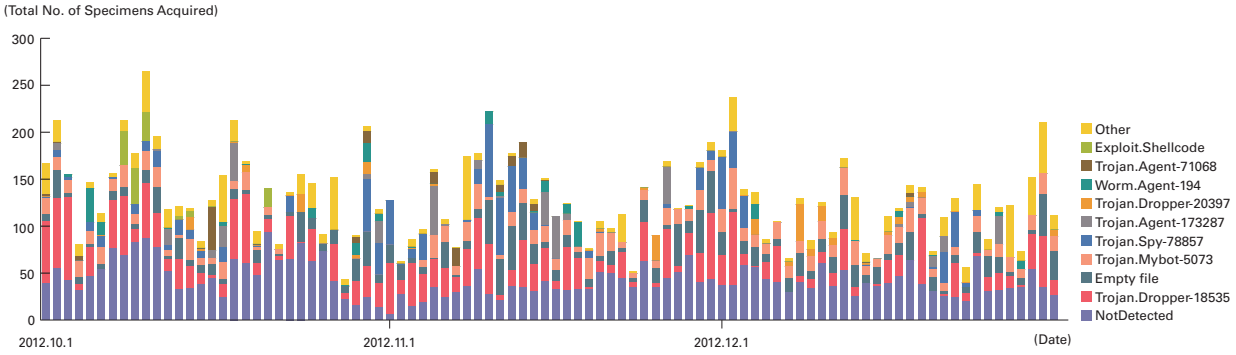

Figure 8: Trends in the Total Number of Malware Specimens Acquired (Excluding Conficker)

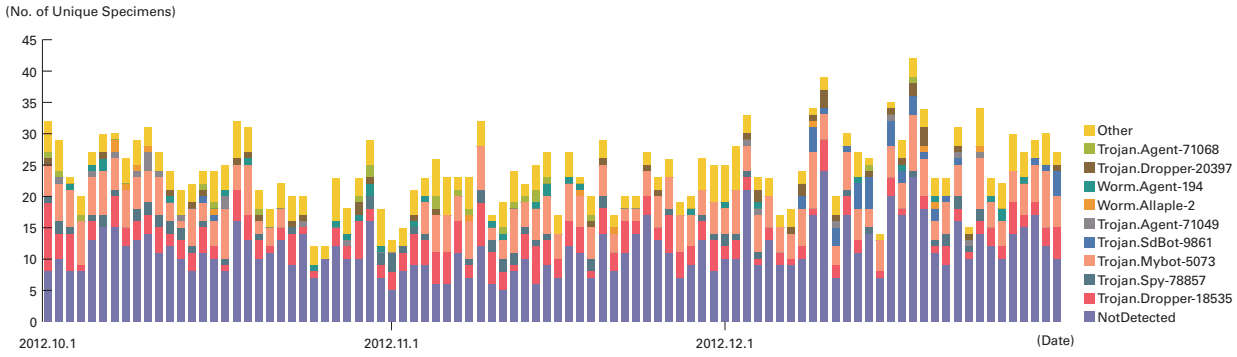

Figure 9: Trends in the Number of Unique Specimens (Excluding Conficker)

*40 This indicates the malware acquired by honeypots.

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

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

On average, 131 specimens were acquired per day during the period under study, representing 24 different malware. The number of specimens acquired has halved compared to the previous report. This may be because the Trojan-Dropper family was comparatively active during the previous survey period, and while it remained active during the current period, the number of specimens acquired halved. Undetected specimens from Thailand and Indonesia also appeared during the current survey period. After investigating these undetected specimens more closely, we learned that two types of bots*42*43 controlled by IRC servers had been active, just as in the past.

Under the MITF's independent analysis, during the current period under observation 71.7% of malware specimens acquired were worms, 25.4% were bots, and 2.9% were downloaders. In addition, the MITF confirmed the presence of 15 botnet C&C servers*44 and 7 malware distribution sites.

■ Conficker Activity

Including Conficker, an average of 41,898 specimens were acquired per day during the period covered by this report, representing 899 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 was about 10% lower than for the previous survey period. Unique specimens were also down by about 6%.

According to the observations of the Conficker Working Group*45, as of December 31, 2012, a total of 1,787,998 unique IP addresses are infected. This is a drop of approximately 47% compared to the 3.2 million PCs observed in November 2011, but it demonstrates that infections are still widespread.

*42 Trojan:Win32/Ircbrute (http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?name=Trojan%3AWin32%2FIrcbrute).
*43 Win32/Hamweq (http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fHamweq).
*44 An abbreviation of Command & Control Server. A server that provides commands to a botnet consisting of a large number of bots.
*45 Conficker Working Group Observations (http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking).

1.3.3 SQL Injection Attacks

Of the types of different Web server attacks, IIJ conducts ongoing surveys related to SQL injection attacks*46. SQL injection attacks have flared up in frequency numerous times in the past, remaining one of the major topics in the Internet security. SQL injections are known to occur in one of three attack patterns: those that attempt to steal data, those that attempt to overload database servers, and those that attempt to rewrite Web content.

Figure 10 shows the distribution of SQL injection attacks against Web servers detected between October 1 and December 31, 2012. Figure 11 shows trends in the numbers of attacks. These are a summary of attacks detected by signatures on the IIJ Managed IPS Service.

Japan was the source for 33.6% of attacks observed, while the United States and Germany accounted for 24.6% and 14.2%, respectively, with other countries following in order. Fewer SQL injection attacks were made against Web servers compared to the previous report. Attacks from the United States rose to second place, and those from Germany rose to 3rd place, due to attacks directed at specific targets that occurred on certain days.

During this period, attacks from specific attack sources in the United States, Germany, and the Netherlands directed at specific targets took place on October 10. Similar attacks were also made on a larger scale on October 26. On December 17, there were attacks from specific attack sources in China directed at specific targets. These attacks are all thought to have been attempts to find vulnerabilities on a Web server.

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

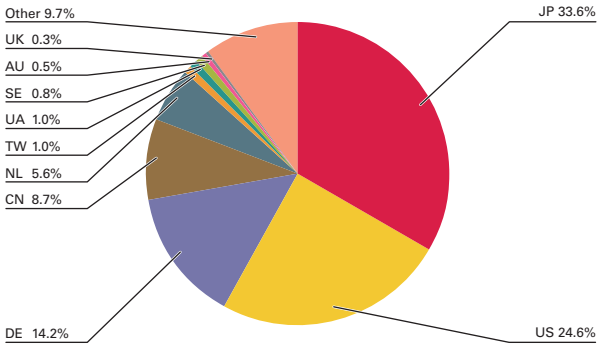

Figure 10: Distribution of SQL Injection Attacks by Source

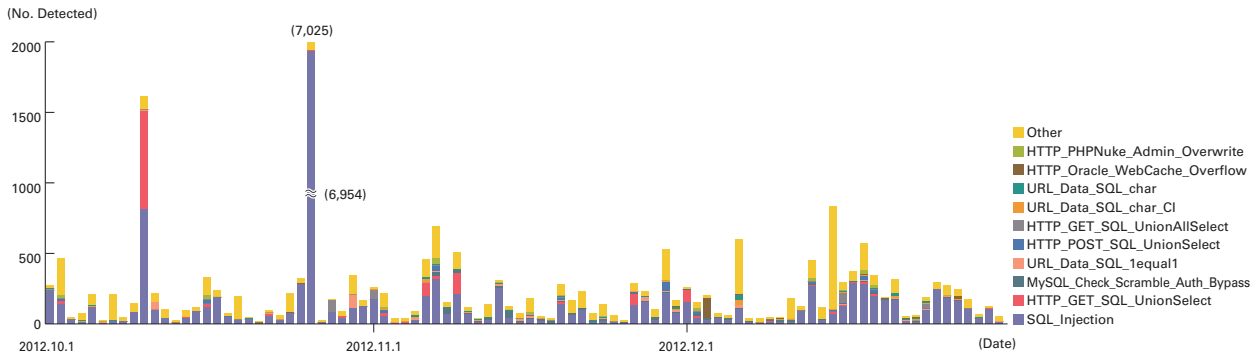

Figure 11: Trends in SQL Injection Attacks (by Day, by Attack Type)

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

1.4 Focused Research

Incidents occurring over the Internet change in type and scope from one minute to the next. Accordingly, IIJ works toward implementing countermeasures by continuing to perform independent surveys and analyses of prevalent incidents. Here, we present information from the survey we have undertaken during this period covering three themes. First, we give an overview of the Tor tool for anonymizing communications. Next, we discuss the Citadel variant of the ZeuS malware, which was used to steal random number tables for authentication from users of financial institutions in Japan. Finally, we reflect on the issues that have been plaguing protocols and implementations based on cryptographic technology, and consider how they should be handled.

1.4.1 An Overview of Tor

Tor is an overlay network*47 built to anonymize communication routes. In around 1995, there were concerns that it was possible to confirm who was communicating with who by analyzing communications, and a United States Navy research facility looked into methods for achieving anonymous connections. They came up with a method for securing the anonymity of a source by installing relay nodes on a network, and routing traffic through a number of these. This method was called onion routing, named for the fact that the packets are wrapped in multiple layers of encryption like the layers of an onion, so that each relay node they are routed through can only read the minimum amount of information necessary. Research continued following this, and the third generation*48 implementation of onion routing developed in about 2002 was given the name Tor. Later, the source code for this was published under the MIT license, and development continued with funding from a variety of organizations. Currently, development of The Tor Project continues with sponsorship from government organizations, NGOs, and an assortment of other groups and individuals.

Tor anonymous connections appear to be used by a wide variety of people. According to The Tor Project, they are used by journalists for safe communication with informants and dissidents, and by NGO staff to connect to their own websites without being detected while working overseas. The United States Navy and law enforcement agencies also use them for gathering intelligence and conducting communications. In countries without freedom of speech, individuals may even put their lives in danger by making statements critical of their government. There are actually some countries in which all communications are apparently monitored, and being able to use anonymous connections in places like these is extremely important for the people living there. For example, the number of users of Tor increased dramatically from around 2011, when the protests known as the Arab Spring became more heated*49. These governments also know of the existence of Tor, and have attempted to implement a variety of filtering technology to prevent its use. In each case, The Tor Project has updated its implementation to make it harder to filter, maintaining an environment in which anonymous connections are available to users.

Currently, approximately 3,000 relay nodes are operated around the world by volunteers and other parties. The Tor client first accesses a directory server based on a list of directory services contained within it, and updates the list of relay nodes. The client then selects three of these relay nodes. These consist of an entry node to the Tor Network, a middle node, and an exit node back to the Internet. The exit node is slightly unique, as each node operator sets the kind of communications they will permit. Even when a node operator allows communications as an exit node, a number of ports are restricted under the standard settings as shown below.

TCP/25 (SMTP), TCP/119 (NNTP), TCP/135-139 (RPC/NetBIOS),
TCP/445 (Microsoft-DS), TCP/563 (NNTPS), TCP/1214 (Kazaa),
TCP/4661-4666 (eDonkey), TCP/6346-6429 (Gnutella), TCP/6699 (Napster, WinMX),
TCP/6881-6999 (BitTorrent)

Node operators can of course allow these communications under their own policies, but the filters are apparently measures to prevent abusive behavior, as well as excessive load on the network due to file sharing. It is also possible to completely

*47 A logical network built on top of another network.
*48 At the time the project was called second generation, but it is equivalent to the third generation if you include the first onion routing implementation.
*49 For example, looking at the graph for Egypt, we can see that users increased from 2010. The graph also shows that users declined to almost zero on January 28, 2011 because Internet communications were shut down, but later recovered. The Tor Project, Inc., "Directly connecting Tor users" (https://metrics.torproject.org/users.html?graph=directusers&start=2010-04-01&end=2013-01-31&country=eg&events=off#direct-users).

disallow external communications on an exit node. The client can determine what kind of exit node communications are allowed by each node, so a node that permits the communications you want to carry out is selected as the exit node.

The client establishes encrypted communications with the initial entry node from among the three nodes selected. Next, it establishes encrypted communications from the entry node to the middle node, and from the middle node to the exit node. After setting up this virtual line from the entry node to the exit node, the client is able to communicate with the server by notifying the exit node to connect to the final target server. During this process the entry node knows which client communications are originating from, but it merely relays this to the middle node, so it doesn't know the final destination of communications. The middle node only knows that communications are taking place between the entry node and exit node. The exit node knows that a request to communicate with the target server has come via the middle node, but it does not know anything more about the source. The target server can only see that a communication request has come from the exit node (Figure 12). This is how onion routing achieves anonymous communications.

The exit node communicates with the server via plain text, so the user must utilize a separate end-to-end encryption protocol such as SSL when they want to guarantee the anonymity of a message.

Attempts to inhibit the use of Tor include methods such as looking up the IP addresses of directory servers and entry nodes, and blocking access to them. Blocks have actually been implemented for some networks. In response, Tor implemented a system called bridge nodes. These are relay nodes that are not advertised, and have the same function as entry nodes. The difference is, they are left off public lists to avoid blocking. Some methods to identify a small number of bridge nodes have been provided, but bridge nodes are managed under a system that prevents the entire list from being referenced. Users can circumvent blocks and utilize anonymous connections through Tor by using these bridge nodes as relays to entry nodes and directory servers (Figure 13).

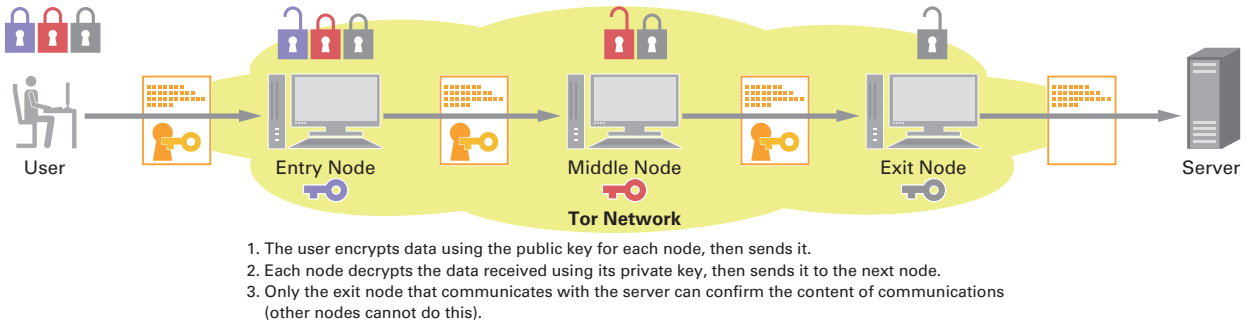

Figure 12: Encryption of Tor Communications

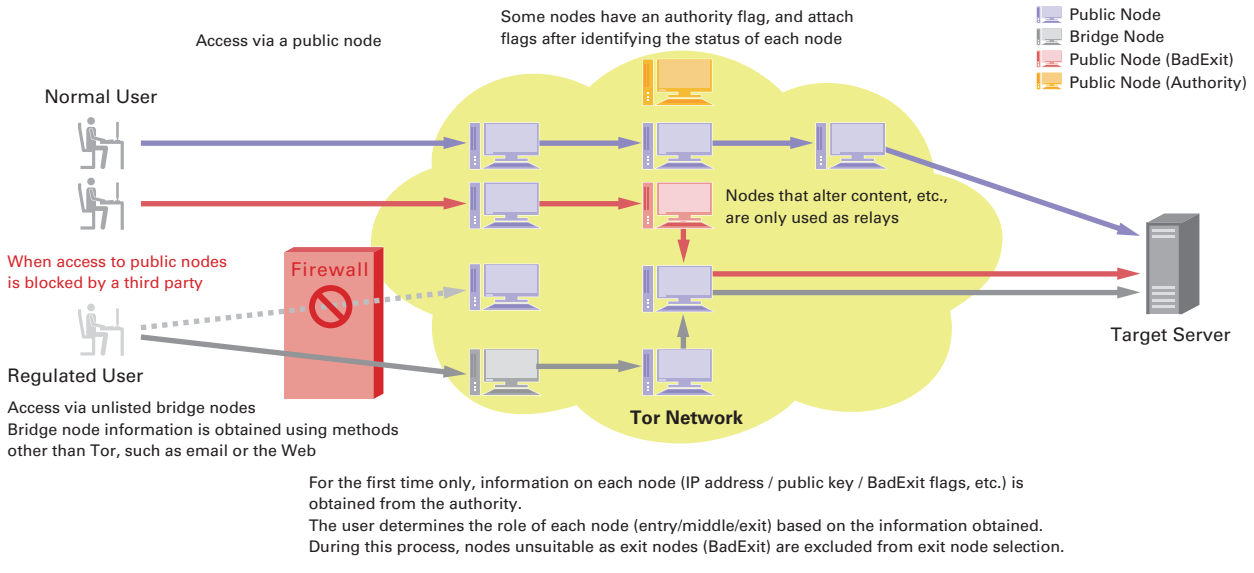

Figure 13: An Overview of Tor

From a network operator's standpoint, Tor communications appear to be taking place between the client and the entry node, the entry node and the middle node, the middle node and the exit node, and the exit node and the server. Unless there is very little network flow, given the current traffic volumes on the Internet, the distribution of relay nodes, and the number of Tor users, even if all communications are monitored, it is difficult to trace how each is related. It is hard to identify users even if relay nodes are operated to intercept communications. The client determines which nodes are used, so this system makes it impossible to intercept specific communications. Even if selected as a relay node by the user by chance, although the user's source IP address can be identified via the entry node, it is not possible to learn the target of communications. Middle nodes do not have access to any meaningful information, and although exit nodes can see the target and content of communications, they cannot identify where the user is communicating from. If the user utilized encrypted communications, it is not even possible to identify the content.

This is how Tor provides anonymous connections to users. Of course, Tor may also be used by criminals. In this case, they have anonymity in the same way as general users who require Tor, and this system makes it difficult to trace criminals. In response to this, The Tor Project states, "Tor aims to provide protection for ordinary people who want to follow the law. Only criminals have privacy right now, and we need to fix that. ...So yes, criminals could in theory use Tor, but they already have better options, and it seems unlikely that taking Tor away from the world will stop them from doing their bad things." As mentioned previously a number of filters have also been implemented for Tor, and its structure makes it difficult to use it for spam, etc. Regarding the potential for using it as a stepping stone for attacks such as DDoS, because relay nodes only relay legitimate TCP connections, typical attack methods such as SYN floods and UDP floods cannot be executed through the Tor Network, although the chance of it being used in connection floods or GET floods remains. The anonymous connection feature of Tor was developed to protect freedom of expression, privacy, and human rights. It is also an essential tool now for many people around the world. IIJ will continue to investigate trends in these implementations and research fields, and strive to achieve a better Internet society.

1.4.2 The Citadel Variant of ZeuS

Citadel is a relatively new malware that appeared between late 2011 and early 2012. It is based on the well-known ZeuS*50 banking Trojan. Like SpyEye*51, it is said that Citadel may have been used in incidents of money-related theft from financial institutions in Japan that occurred in 2012*52. IIJ obtained Citadel specimens itself, and compared it with the original ZeuS to see how it has been changed, while also investigating Citadel-related incidents.

■ An Overview of Citadel

ZeuS, which Citadel is based on, is a crimeware kit like SpyEye that is designed to steal authentication information for financial institutions, and ultimately make financial gain. Its main functions are the alteration of Web content on the browser of an infected computer*53, as well as the theft of authentication information saved to or entered into browsers or FTP clients, and authentication information from FTP or POP3 communications. Another of its characteristics is the wide range of variants that exist*54.

*50 See "1.4.3 ZeuS and its Variants" in Vol.16 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol16_EN.pdf) for more information on ZeuS.

*51 See "1.4.2 SpyEye" in Vol.13 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol13_EN.pdf) for more information on SpyEye.

*52 For example, the Symantec blog reported that ZeuS variants targeting financial institutions in Japan had been discovered. "Zeus Now Setting its Sights on Japanese Online Banking Customers" (http://www.symantec.com/connect/blogs/zeus-now-setting-its-sights-japanese-online-banking-customers).

*53 A system for stealing information by altering HTTP or HTTPS Web content. For example, information is stolen by inserting HTML that prompts a user to enter all the numbers listed on the random number table provided as two-factor authentication on the authentication page for Internet banking, etc. Attackers can later use this information to steal money. When communications are encrypted using HTTPS, attacks are made by altering or stealing the outgoing data before it is encrypted, or the incoming data directly after it is decrypted.

*54 For example, a ZeuS variant operating in tandem with smartphone-based malware was used to break the two-factor authentication called mTAN (mobile transaction authentication number), which is often used for Internet banking in Europe. See the following McAfee blog post for more details. "Spitmo vs Zitmo: Banking Trojans Target Android" (http://blogs.mcafee.com/mcafee-labs/spitmo-vs-zitmo-banking-trojans-target-android). There are a wide variety of other variants, such as those with functions for conducting DoS attacks as a bot.

Because Citadel is based on ZeuS, it has all the same basic functions. Compared to the original ZeuS, it implements a function for reading expansion modules, a number of new bot commands, a function for altering DNS responses, and a function for stealing information from relatively new environments such as Google Chrome. It also has a function for immediately updating the WebInject config, and a function for preventing analysis via detection in virtual or sandbox environments. Another interesting function is that it is designed to not operate in Russian or Ukrainian language environments (keyboard settings). At the time of writing it is about a year since Citadel was discovered, and it is under active development. For example, compared to Citadel 1.3.4.5 that was released in June of 2012, version 1.3.5.1 that was confirmed about four months later supports a number of new bot commands, and a variety of other functions have been added or enhanced*55. Figure 14 shows a list of each function executed with the corresponding bot command. The functions added since ZeuS 2.0.8.9 have red borders. These include the previously mentioned "module_*" for reading expansion modules, "dns_filter_*" for altering DNS responses, and "webinjects_update" for immediately updating the config for WebInject (alteration of Web content in a browser).

IIJ found that when comparing the code for version 2.0.8.9 of the original ZeuS and version 1.3.5.1 of Citadel that we obtained ourselves, approximately 60% of the functions were almost perfect matches. After implementing code analysis, the newly added parts also matched the previously mentioned characteristics of Citadel, and although there were minor differences in encryption algorithms, it was clear that the ZeuS code was mostly reused for the basic functions. This demonstrates that the author of Citadel focused on incorporating expansion functions and enhancing functions for stealing authentication information, without making major changes to the basic functions of ZeuS.

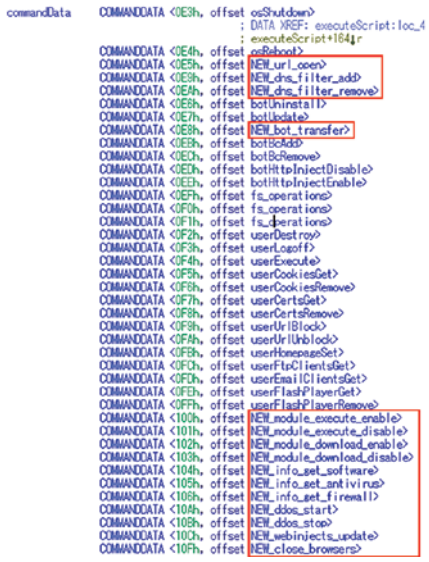

Figure 14: Function Table Corresponding to Citadel Bot Commands

■ Incidents Utilizing Citadel

In August 2012, the FBI issued a warning regarding the Citadel framework, as well as ransomware*56 installed additionally by Citadel*57. This shows that in addition to seizing authentication information for financial institutions, attackers were also attempting to steal more money using the function for reading expansion modules that was added to Citadel.

There has also been an incident in which an attacker used Citadel to hack the employee VPN at an airport*58. Generally, incidents using crimeware kits are aimed at stealing authentication information or money. However, in this incident, the attacker targeted infrastructure rather than financial gain. Because of this, it is thought that the attacker's ultimate goal was not to steal money, and this point makes it an interesting incident. From this we can see that Citadel is merely a tool, and it can cause a variety of harm depending on the goals of the attacker.

*55 The main functions of Citadel 1.3.4.5 and 1.3.5.1 are explained in detail in the following blog posts. "Inside Citadel 1.3.4.5 C&C & Builder - Botnet Control Panel" (http://malware.dontneedcoffee.com/2012/07/inside-citadel-1.3.4.5-cncNbuilder.html) "Update to Citadel : 1.3.5.1 Rain Edition. "(http://malware.dontneedcoffee.com/2012/10/citadelupdate1.3.5.1.html).

*56 Ransomware is malware that encrypts some or all files or disk drives, taking them hostage and preventing the user from accessing important data unless demands for payment are met. Malicious varieties include those that use public key encryption methods so they cannot be decrypted by simply analyzing the malware, as well as those that destroy files while stating that they are just encrypted, demanding money even though decryption is not possible.

*57 The FBI issued a warning regarding Citadel and the ransomware that it also installs in August 2012. "Citadel Malware Continues to Deliver Reveton Ransomware in Attempts to Extort Money" (http://www.fbi.gov/sandiego/press-releases/2012/citadel-malware-continues-to-deliver-reveton-ransomware-in-attempts-to-extort-money).

*58 The airport VPN hacking incident was reported in the following Trusteer Blog. "Citadel Trojan Targets Airport Employees with VPN Attack" (http://www.trusteer.com/blog/citadel-trojan-targets-airport-employees-with-vpn-attack).

In Japan, incidents of monetary theft using a ZeuS variant thought to be Citadel as well as SpyEye were reported at financial institutions including major banks between October and November 2012. The characteristic of these incidents was that authentication information was seized by displaying a pop-up that prompted users to enter all the numbers listed on their two-factor authentication card. This method had been confirmed in places such as Brazil in the past. For example, there were incidents in which these techniques were employed by phishing sites and the malware known as Bancos*59. With incidents of monetary theft using SpyEye occurring in 2011, the fact that the IPA has issued an alert*60, and money stolen*61 due to spyware infections in at least 2005, it can be said that such incidents are occurring in Japan on a routine basis, and are not limited to the incidents discussed here.

■ Infection Vectors

It is known that drive-by downloads*62 using exploit kits*63 such as the Blackhole Exploit Kit*64 are common infection vectors for Citadel. Like Gumblar*65, this involves a variety of techniques, such as redirecting users to a malicious site by altering legitimate website content, or social engineering methods that prompt users to click a URL in an SNS message or email.

■ Countermeasures

As indicated previously, Citadel can have a different impact depending on the goal of the attacker, but here we consider measures preventing the exploitation of financial institutions. First, if the website you are using provides a one-time password, this should be used*66. Also, when a financial institution provides a service for notifying users by email when you log in or conduct transactions, use of this can help the early detection of damages.

The random number table provided by financial institutions as two-factor authentication lists different numbers for each user. This system reduces exploitation through identity theft when a password is stolen, as it is possible to reaffirm the identity of a user by requiring that several of these numbers selected at random are entered for each transaction. This means that users will never normally be required to enter all the numbers at once. Users can catch abnormalities like this by understanding the purpose of the functions that are provided when using them. It is also important for financial institutions to continue to educate users on the original purpose of these functions, and constantly enhance measures for dealing with threats. As with monetary theft due to malware infections, damages caused by phishing are still being reported*67. As always, it is crucial to check the URL and server certificate (X.509) for websites you communicate with to confirm that they are legitimate. However, when infected with malware such as Citadel or SpyEye, it is difficult to notice abnormalities using existing phishing countermeasures, because malware code injected into Web browsers alters the Web content within them (Figure 15). For this reason, it is important to protect yourself against malware infections.

*59 For example. the following CAIS page shows images used in incidents in which two-factor authentication information was seized using these methods. The incidents occurred at phishing sites targeting Brazilian banks in at least 2009. “Fraudes identificadas e divulgadas pelo CAIS” (http://www.rnp.br/cais/fraudes.php?id=2261&ano=&mes=&pag=52&busca=&tag_extend=&tag=3) (in Portuguese).

*60 In August 2011, IPA reported in its “Computer Virus/Unauthorized Computer Access Incident Report - August 2011 - ” (http://www.ipa.go.jp/security/english/virus/press/201108/documents/summary1108.pdf) that SpyEye was active in Japan with money having been stolen between June and July of 2011, and issued an alert. IBM’s Tokyo SOC Report also mentioned that SpyEye was active in Japan. “An increase in the number of SpyEye viruses detected” (https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/spyeye_20110425?lang=ja) (in Japanese), “An increase in the number of SpyEye viruses detected (continued)” (https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/spyeye_20110817?lang=ja_jp) (in Japanese).

*61 For example, IPA issued the following alert in July 2005 due to the circulation of spyware that targeted users of Internet banking services operated by financial institutions in Japan. “A Warning for Preventing Harm due to Spyware” (http://www.ipa.go.jp/security/topics/170720_spyware.html) (in Japanese).

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

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

*64 The relationship between Citadel and the Blackhole exploit kit is explained in the following articles. “Citadel 1.3.5.1 Rain Edition” (http://www.xylibox.com/2012/10/citadel-1351-rain-edition.html), Context INFORMATION SECURITY, “Malware - Exploit Packs, Zeus and Ransomware” (http://www.contextis.com/research/blog/malware-exploit-packs-zeus-and-ransomware/).

*65 See “1.4.2 ID/Password Stealing Gumblar Malware” in Vol.4 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol04_EN.pdf) and “1.4.1 Renewed Gumblar Activity” in Vol.6 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol06_EN.pdf) for more information on Gumblar.

*66 It is difficult to completely eliminate this type of attack even when two-factor authentication is used. McAfee reported that money was actually stolen in an environment using a smart card reader in Operation High Roller. “Dissecting Operation High Roller” (http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf). However, because security is greatly improved compared to two-factor authentication using random number tables, it is still best to use one-time passwords if they are provided by a financial institution.

*67 For example, the Council of Anti-Phishing Japan issued several alerts in 2012 for financial institutions in Japan. “Council of Anti-Phishing Japan - Emergency News Bulletin” (http://www.antiphishing.jp/news/alert/) (in Japanese).

To prevent infections, it is important to conduct conventional general security measures thoroughly, such as applying patches to the OS and third-party applications (including browser plug-ins), deleting applications and browser plug-ins that aren't needed, installing the latest version of anti-virus software, and keeping definition files up to date. Additional measures to take that drastically reduce the risk of infection are installing a vulnerability mitigation tool such as EMET*68, and properly conducting policy settings for standard Windows functions such as UAC or AppLocker, or Software Restriction Policies. Other measures for preventing infections through deception by social engineering methods include taking care when opening links or attachments, checking that files are being downloaded from the correct site, and confirming that extensions for downloaded files aren't mislabeled.

1.4.3 A Reflection on Issues Plaguing Protocols and Implementations Using Cryptographic Technology, and the Way Forward

In this section, we discuss a rash of issues with protocols and implementations using cryptographic technology that have been occurring in recent years.

Attacks targeting PKI were made on a number of organizations between 2011 and 2012, such as the fraudulent issue of certificates. In particular, we have learned that the case of fraudulently obtained certificates used with the Flame malware that was discovered in May 2012 was a high level attack caused by a combination of technological and operational factors. For this reason, some have noted that a large number of attacks are potentially already taking place behind the scenes. This has eroded trust in PKI and the trust anchors provided by vendors, leading to a situation in which applications or browsers once recognized as secure can no longer be trusted.

In light of this, in this section we discuss and categorize cases in which protocols and implementations "thought to have been secure were actually not" to find common denominators, and discuss using this information to prevent issues that could occur in the future. We consider different stakeholders such as designers/implementers/operators and users, and attempt to determine a policy for dealing with the attacks expected in the future from each of these perspectives.

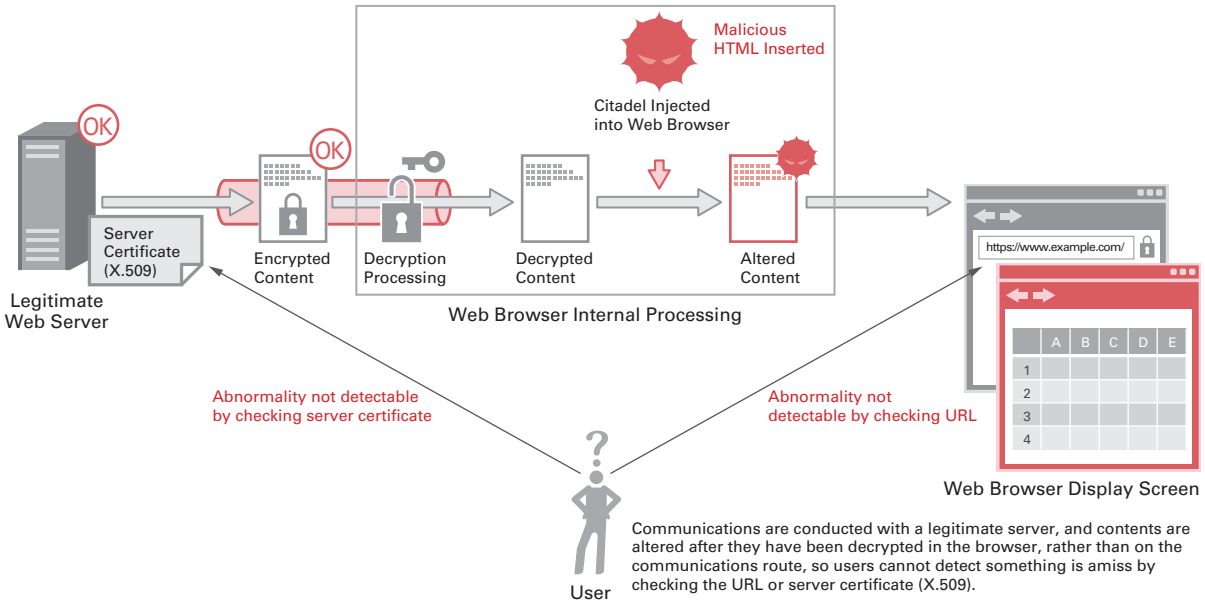

Figure 15: Alteration of Content Inside a Browser by Malware

*68 EMET (Enhanced Mitigation Experience Toolkit) is a tool provided by Microsoft for mitigating the exploitation of vulnerabilities (http://support.microsoft.com/kb/2458544/).

Summarizing Cases in Which Protocols and Implementations Thought to be Secure Were Not

Table 1 classifies vulnerabilities in protocols and implementations using cryptographic technology, as well as incidents caused by these vulnerabilities in the past few years. In addition to issues originating from cryptographic compromises, issues in each of the design/implementation/operation phases are also classified. Of these, issues considered to originate from multiple causes are classified under the main cause. For example, the Flame malware is a case with multiple contributing factors and caused by operational issues in addition to the main cause, which is the compromise of the MD5 algorithm.

Table 1: Classification of Vulnerabilities in Protocols/Implementations Using Cryptographic Technology and Resulting Incidents

Type of Issue	Month/Year	Vulnerability/ Incident Name	Details	Footnote No.
Issue caused by cryptographic compromise	March 2007	APOP password recovery attack	It was disclosed that identity theft attacks on servers were possible by sending a challenge using an MD5 collision attack.	*69, *70, *71
	December 2009	X.509 intermediate CA certificate forgery	Forgery of X.509 intermediate CA certificates was carried out by adjusting the X.509v3 extension area ignored by the browser to make MD5 digests collide. An operational issue that made it possible to infer affected signature data because the certificate serial numbers were issued in increments was also identified.	*72
	January 2010	Factoring of a 768-bit RSA public key	Breaking the previous record of 663-bit encryption, it was reported that a 768-bit RSA public key was successfully factored in approximately six months using 80 machines. 1024-bit RSA is still not a realistic target for attacks, but this was a trigger in moves to transition to 2048-bit RSA.	*73
	May 2012	Flame malware	MITM attacks on Windows Update by using malware to exploit the code-signing function were discovered. Fake Microsoft certificates were issued using MD5 collision attacks.	*74
	August 2012	Padding oracle attack on PKCS#1 v1.5 encryption	An improved method for existing padding oracle attacks on PKCS#1 v1.5 encryption was disclosed. This is a practical attack that appropriates the encryption key from hardware with a PKCS#11 encryption key import function implemented.	*75, *76
	August 2012	Restriction of RSA keys less than 1024 bits in length	Updates were released for the Microsoft family of products that restricted the use of certificates using RSA keys less than 1024 bits in length.	*77
Design issue	November 2008	Key recovery attack on WPA	An attack that allowed the leak of MIC keys and the generation of altered packets due to an issue in the TKIP (Temporal Key Integrity Protocol) key update algorithm for WPA (Wi-Fi Protected Access) was disclosed.	*78
	November 2008	Partial leak of encrypted text via SSHv2 eavesdropping	An attack that leaked the first 4 bytes of a packet when using SSHv2 in CBC mode was disclosed. Using trial-and-error with a system for checking packet length, it has a success rate of 2^{-14}.	*79
	November 2009	SSL/TLS renegotiation vulnerability	A MITM attack that allowed injection into HTTPS fragments via the renegotiation mechanism for refreshing keys and algorithm agreement was disclosed.	*80, *81
	October 2010	Issue when using CBC with IPsec	An attack was disclosed that focuses on the characteristics of the data structure of plain text data called an ESP trailer, which is padded to block size length.	*82
	September 2011	BEAST attack	A tool that obtained cookies within a browser through a chosen plaintext attack on the CBC mode of browsers using SSL 3.0/TLS 1.0 was released.	*83, *84, *85
	October 2011	XML encryption vulnerability (when using CBC mode)	An attack that uses a Web server for returning different error codes according to XML syntax validation errors as a plaintext validity oracle was disclosed.	*86
	December 2011	Issue when using truncated HMAC with TLS1.2	It was pointed out that plain text data may leak with extension methods that use 80-bit truncated data as MACs instead of the usual HMAC as a message authenticator. This applies when the application data for encryption is short and encrypted data is less than the block size.	*87
	July 2012	Release of MS-CHAPv2 decryption tool	A tool was released that can be used from the cloud in attacks on MS-CHAPv2, which was reported by Bruce Schneier in 1999.	*88
	September 2012	CRIME attack	A demo for eavesdropping cookies when the compression function is enabled for SSL/TLS was released. This method rebuilds encrypted data by trial and error. It exploits the fact that even when data of the same length is compressed, the dictionary length changes based on whether the same characters are included in the data before compression.	*89, *90
	September 2012	Password extraction attack in Oracle DB	An attack that could be used to obtain Oracle Database passwords was disclosed. This is also recognized as an issue with authentication protocol design.	*91
Implementation issue	May 2008	Issue with predictable random number generation in Debian's OpenSSL	An issue was disclosed with the fact that private keys were derived from a greatly reduced key space when generating keys using OpenSSL in certain versions of Debian.	*92
	February 2012	Shared public key issue	Two independent groups reported that when public key certificates used with SSL/TLS and SSH, DSA signatures, and PGP keys were collected via extensive scans of IPv4 addresses on the Internet, many unintentionally shared private keys with other sites.	*93, *94
	October 2012	SSL implementation issue in Android apps	The existence of Android apps vulnerable to MITM attacks due to problems with the implementation of SSL was pointed out.	*95
	November 2012	Issue with the implementation of Huawei brand wifi products	It was revealed that session keys that should be selected randomly were hard-coded for the symmetric key cryptography DES used during communications.	*96
Operational issue	March to November 2011	Hacking of multiple certificate authorities and issuing of fraudulent certificates	It was discovered that nine certificates had been issued fraudulently in the Comodo incident in March, and over 500 certificates had been issued fraudulently from DigiNotar in late August. In November a Dutch certificate authority service operated by KPN suspended the issuing of certificates due to the discovery of evidence that their certificate issuing system had been hacked.	*97
	September 2011	Revocation of certificates from 512-bit RSA certificate issuing CA	A policy of revoking certificates from intermediate CAs was taken due to problems with the issuing policy of DigiCert Sdn. Bhd.	*98
	August 2012	Adobe certificate revocation	A code signing certificate used by Adobe was revoked when its fraudulent use was discovered (classified as an operational issue, as currently there has been no follow-up about the cause of the incident).	*99
	October 2012	Use of 512-bit RSA keys for public keys used with DKIM	The DKIM system for authenticating the sender of email requires the use of keys with a length of at least 1024 bits by specification, but it was reported that 512-bit keys had been used.	*100
	October 2012	Compatibility issue affecting signed Microsoft binaries	It was discovered that a number of binaries signed between July 12 and August 14, 2012, were signed based on incorrect procedures. This was due to the code signing certificate not containing Extended Key Usage with regard to time stamping.	*101
	December 2012	Fraudulent issue of certificates from the TURKTRUST certificate authority	It was discovered that a number of certificates for domains such as *.google.com had been fraudulently issued from the TURKTRUST certificate authority.	*102, *103

The compromise of cryptographic algorithms*[104] indicates that their security can be threatened at a lower cost than envisioned when they were designed. It is caused by a drop in the cost of attacks through increases in CPU processing power or the use of cloud computing, as well as advancements in cryptanalysis research. This means the degradation of algorithms over time is unavoidable, and it will be necessary to migrate from the algorithms currently used to new algorithms at some point. We can see that some of the vulnerabilities listed in Table 1 are caused by the use of hash function MD5 or the RSA algorithm with a comparatively short key length. These vulnerabilities can be dealt with comprehensively by migrating from MD5 to the SHA-2 family*[105], or shifting to the use of RSA public keys with a length of 2048 bits or more.

*69 Gaetan Leurent, "Message Freedom in MD4 and MD5 Collisions Application to APOP", FSE2007 (http://fse2007.uni.lu/slides/APOP.pdf).
*70 Yu Sasaki, Go Yamamoto, Kazumaro Aoki, "Practical Password Recovery on an MD5 Challenge-Response such as APOP", FSE2007 Rump session (www.iacr.org/workshops/fse2007/slides/rump/apop.pdf).
*71 Yu Sasaki, Lei Wang, Kazuo Ohta, Noboru Kunihiro, "Extended Password Recovery Attacks against APOP, SIP, and Digest Authentication", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E92-A No.1, pp.96-104.
*72 Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, Benne de Weger, "MD5 considered harmful today" (http://www.win.tue.nl/hashclash/rogue-ca/).
*73 Thorsten Kleinjung et.al, "Factorization of a 768-bit RSA modulus" (http://eprint.iacr.org/2010/006).
*74 See "1.4.2 The Flame Malware that Launches MITM Attacks on Windows Update" in Vol.16 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol16_EN.pdf).
*75 Romain Bardou, Riccardo Focardi, Yusuke Kawamoto, Lorenzo Simionato, Graham Steel, Joe-Kai Tsay, "Efficient Padding Oracle Attacks on Cryptographic Hardware", CRYPTO2012 (http://www.lsv.ens-cachan.fr/~steel/slides/CRYPTO12.pdf).
*76 Efficient Padding Oracle Attacks on Cryptographic Hardware FAQ (http://www.lsv.ens-cachan.fr/~steel/efficient-padding-oracle-attacks/faq.html).
*77 Microsoft, TechNet Blogs "An update (KB2661254) for blocking cryptographic keys less than 1024 bits in length was released in August 14" (http://blogs.technet.com/b/jpsecurity/archive/2012/07/30/3511493.aspx) (in Japanese).
*78 Erik Tews, "Gone in 900 Seconds, Some Crypto Issues with WPA", PacSec2008.
*79 CERT/CC, "Vulnerability Note VU#958563 SSH CBC vulnerability" (http://www.kb.cert.org/vuls/id/958563).
*80 MITRE, CVE-2009-3555 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555).
*81 E. Rescorla, M. Ray, S. Dispensa, N. Oskov, "Transport Layer Security (TLS) Renegotiation Indication Extension" (http://www.ietf.org/rfc/rfc5746.txt).
*82 Jean Paul Degabriele, Kenneth G. Paterson, "On the (In)Security of IPsec in MAC-then-Encrypt Configurations", the 17th ACM conference on Computer and communications security (ACM CCS2010) (http://www.isg.rhul.ac.uk/~psai074/slides/CCS-2010.pdf).
*83 Qualys Security Labs, "Mitigating the BEAST attack on TLS" (https://community.qualys.com/blogs/securitylabs/2011/10/17/mitigating-the-beast-attack-on-tls).
*84 Microsoft, MSDN Blogs, "Fixing the BEAST" (http://blogs.msdn.com/b/kaushal/archive/2012/01/21/fixing-the-beast.aspx).
*85 CRIME vs startups (http://www.youtube.com/watch?v=gGPhHYyg9r4).
*86 Tibor Jager, Juraj Somorovsky, "How to Break XML Encryption", the 18th ACM Conference on Computer and Communications Security (ACM CCS2011) (http://www.nds.rub.de/media/nds/veroeffentlichungen/2011/10/22/HowToBreakXMLenc.pdf).
*87 IIJ-SECT Security Diary, "Regarding a Vulnerability When Using Truncated HMAC with TLS1.2" (https://sect.iij.ad.jp/d/2011/12/079269.html) (in Japanese).
*88 CloudCracker::Blog, "Divide and Conquer: Cracking MS-CHAPv2 with a 100% success rate" (https://www.cloudcracker.com/blog/2012/07/29/cracking-ms-chap-v2/).
*89 Juliano Rizzo, Thai Duong, "The CRIME attack", ekoparty Security Conference 2012 (http://www.ekoparty.org/eng/2012/thai-duong.php).
*90 CRIME: Information Leakage Attack against SSL/TLS (https://community.qualys.com/blogs/securitylabs/2012/09/14/crime-information-leakage-attack-against-ssltls).
*91 Esteban Fayo, "Cryptographic flaws in Oracle Database authentication protocol", ekoparty Security Conference 2012 (http://www.ekoparty.org/eng/2012/esteban-fayo.php).
*92 Debian Security Advisory, "DSA-1571-1 openssl -- predictable random number generator" (http://www.debian.org/security/2008/dsa-1571).
*93 See "1.4.1 The Issue of Many Public Keys Used with SSL/TLS and SSH Sharing Private Keys with Other Sites" in Vol.17 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol17_EN.pdf).
*94 Yuji Suga, The Issue of Many Public Keys Unintentionally Sharing Private Keys with Other Sites, JNSA PKI Day 2012 (http://www.jnsa.org/seminar/pki-day/2012/data/PM02_suga.pdf) (in Japanese).
*95 Martin Georgiev, Subodh Iyengar, Suman Jana, Rishita Anubhai, Dan Boneh, Vitaly Shmatikov, "The Most Dangerous Code in the World: Validating SSL Certificates in Non- Browser Software", the 19th ACM Conference on Computer and Communications Security (ACM CCS2012) (http://www.cs.utexas.edu/~shmat/shmat_ccs12.pdf).
*96 Roberto Paleari, Ivan Speziale, "Weak password encryption on Huawei products" (http://blog.emaze.net/2012/11/weak-password-encryption-on-huawei.html).
*97 See "1.4.3 Incidents of the Unauthorized Issue of Public Key Certificates" in Vol.13 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol13_EN.pdf).
*98 See "1.4.1 Problems Related to the Issuing of Public Key Certificates" in Vol.14 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol14_EN.pdf).
*99 Adobe Secure Software Engineering Team (ASSET) Blog, "Inappropriate Use of Adobe Code Signing Certificate" (https://blogs.adobe.com/asset/2012/09/inappropriate-use-of-adobe-code-signing-certificate.html).
*100 US-CERT, "Vulnerability Note VU#268267, DomainKeys Identified Mail (DKIM) Verifiers may inappropriately convey message trust" (http://www.kb.cert.org/vuls/id/268267).
*101 Microsoft, "Microsoft Security Advisory (2749655) Compatibility Issues Affecting Signed Microsoft Binaries" (http://technet.microsoft.com/en-us/security/advisory/2749655).
*102 Microsoft, "Microsoft Security Advisory (2798897): Fraudulent Digital Certificates Could Allow Spoofing" (http://technet.microsoft.com/en-us/security/advisory/2798897).
*103 TÜRKTRUST, "Kamuoyu Açıklaması" (http://www.turktrust.com.tr/kamuoyu-aciklamasi.html) (in Turkish).
*104 See "1.4.1 Trends in the Year 2010 Issues on Cryptographic Algorithms" in Vol.8 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol08_EN.pdf).
*105 Official Announcement of "List of Recommendable Cryptographic Techniques for Procurement Activities by Japan e-Government (CRYPTREC Ciphers List)"(http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/130301_01.html), which was open for public comment until January 2013, SHA-1 was accepted for continued use to maintain compatibility, and SHA-256/384/512 was recommended as its replacement.

Next, we consider guidelines for dealing with the design and implementation issues. Many of the vulnerabilities classified as design issues in Table 1 correspond to techniques for leaking internal information a bit at a time by observing the response (external information) when repeating trial and error. In particular, padding oracle attacks on CBC mode*106 involve an issue identified by Serge Vaudenay in 2002, and we know that this issue now presents a real threat due to improvements and extensions in the past few years.

Techniques for reconstructing plain text at random by observing responses from an actual server targeted in an attack and making multiple trial and error attempts have been applied to SSL/TLS*83*87, IPsec*79, SSH*82 and the XML Encryption specification*86. The basic idea behind these techniques is to see whether the responses from nodes targeted in an attack have correct padding data or not and extract information bit-by-bit, as identified by Vaudenay. This trial and error concept is also used in key recovery attacks on WPA*78 and CRIME attacks*89. In view of the fact that these issues are caused by poor error processing rather than normal processing, we can see that there is a need to carry out protocol design. It is clear that this is also an issue that should be taken into consideration for implementation.

The Formation of a New Academic-Industrial Alliance

A side channel attack is a technique for cryptanalysis. This method obtains information such as the keys used in cryptographic processing by collecting secondary information such as deviations in power, electromagnetic waves, or processing speed on a cryptographic chip level. The trial and error analysis technique mentioned previously differs only in the scope of data collected, and is basically based on the same concept. The development of side channel attacks has had a significant impact on cryptographic algorithm design and the establishment of secure implementation methods. In the future, there is a chance that this knowledge can be applied to protocol or format design. For this reason, instead of completely separating cryptographic algorithm design and protocol design, we need a scheme that conveys points requiring caution and issues regarding the use of encryption to protocol designers and implementers. Many excellent, balanced cryptographic algorithms with provable security and high performance have been proposed. However, there have also been cases in which the overall security as a protocol or system is not maintained due to design flaws and implementation issues when using them. There have also been many instances in which the security provided is worlds apart from that envisioned when the algorithm was designed, due to random numbers being generated without enough entropy. This applies to incidents such as a vulnerability in Debian's OpenSSL*92, the issue of public key sharing*93, and the disclosure of an MS-CHAPv2 attack tool*88.

In light of this situation, there have been moves to share the real-world challenges faced by cryptographic technology between the scientific and business communities. For example, workshops*107*108 have been held due to concerns by the scientific community. A workshop for correctly understanding the vulnerabilities relating to CBC mode that we mentioned earlier was held in Japan in March 2013. It is hoped that activities such as these will promote the sharing and understanding of issues, and lead to fundamental solutions.

We believe that this new academic-industrial alliance should place particular focus on enhancing the visibility of the impact of vulnerabilities. Current attempts to quantify the impact of vulnerabilities include the Common Vulnerability Scoring System (CVSS)*109. However, the actual impact is greatly influenced by the prerequisites and usage environment for an attack, so right now it is used as a single reference point. For example, the BEAST attack*83 was evaluated as a MEDIUM vulnerability with a CVSS base score of 4.3*110, but because of factors such as not being able to connect to servers with countermeasures in place, there was a lot of confusion. This is thought to stem from the fact that this evaluation does not calculate the impact of migration in addition to the vulnerability itself. For this reason, we believe there is a need for evaluation standards related

*106 Serge Vaudenay, "Security Flaws Induced by CBC Padding Applications to SSL, IPSEC, WTLS...", EUROCRYPT2002 (http://www.iacr.org/archive/eurocrypt2002/23320530/cbc02_e02d.pdf).

*107 The Workshop on Real-World Cryptography (https://crypto.stanford.edu/RealWorldCrypto/index.php) was held in January 2013. The previous incarnation of this workshop, Is Cryptographic Theory Practically Relevant? (http://www.newton.ac.uk/programmes/SAS/sasw07.html) was held in January 2012.

*108 The 1st Workshop on Real-Life Cryptographic Protocols and Standardization (http://www.nec.com/en/global/rd/event/RLCPS10.html) was held in January 2010, and The 2nd Workshop on Real-Life Cryptographic Protocols and Standardization (http://www.nec.com/en/global/rd/event/RLCPS11.html) was held in March 2011.

*109 P.Mell, K.Scarfone, S.Romanosky, "A Complete Guide to the Common Vulnerability Scoring System (CVSS) Version 2.0" (http://www.first.org/cvss/cvss-guide.pdf). See the following Information-Technology Promotion Agency, Japan Security Center explanation for more information (http://www.ipa.go.jp/security/vuln/CVSS.html) (in Japanese).

*110 NIST, "CVSS Version 2 Scoring Page (CVE-2011-3389)" (http://nvd.nist.gov/cvss.cfm?version=2&name=CVE-2011-3389&vector=%28AV%3AN/AC%3AM/Au%3AN/C%3AP/I%3AN/A%3AN%29).

to migration cost that can be applied to protocol/format specification vulnerabilities. They should use a concept similar to equivalent strength*104, which uses the same grading scale for different types of cryptographic algorithms so they are treated uniformly independent of OS or platform. These standards should also be capable of handling cryptographic compromises. It is expected that sharing common issues and methodology concerning migration and gathering information on examples of successes and failures will serve as a wellspring offering a fresh perspective on the creation of "transition engineering".

Increasing User Awareness

Next, we look at guidelines regarding countermeasures for operators and users. All the incidents listed as operational issues in Table 1 are related to PKI. These issues are caused by a wide range of factors on the operational side, such as vulnerabilities in certificate issuing systems, misuse of certificate attributes, and the erroneous use of cryptographic algorithms with short key lengths. Due to a series of issues occurring in quick succession, a specification of baseline requirements*111 was put into effect from July 2012. These are expected to equalize the variation in issuing requirements between each certificate authority, raise the level of the industry as a whole, and restore confidence in PKI.

However, there have also been unfortunate incidents that serve to erode trust in PKI, such as the discovery that certificates had been issued fraudulently from the TURKTRUST certificate authority in December 2012. PKI offers trust anchors for users, and if trust in PKI is lost through issues such as the fraudulent issuing of certificates, it will develop into a major problem, with browsers no longer able to tell the difference between legitimate sites and malicious sites. Measures such as DANE*112 or Convergence*113 that create new trust anchors to complement the existing PKI system have been proposed to deal with these issues. Using these will redefine the idea that as long as the padlock icon appears in a browser you are safe, and will enable users to raise the security of communications using other trustworthy systems. We believe there should be discussion about how to spread the new concept that users can ensure other trust anchors by themselves and who will cover the cost of raising awareness.

1.5 Conclusion

This report has provided a summary of security incidents to which IIJ has responded. This time, we examined the Tor system that attracted attention due to its connection to the "Remote Control Virus", as well as the Citadel variant of ZeuS that was used to steal code tables for financial institutions. We also discussed the causes behind of a rash of issues in environments using cryptographic technology. IIJ makes every effort to inform the public about the dangers of Internet usage by identifying and publicizing incidents and associated responses in reports such as this.

Authors:

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

Hirohide Tsuchiya, Hisao Nashiwa (1.2 Incident Summary)
Hirohide Tsuchiya, Hiroshi Suzuki, Hisao Nashiwa (1.3 Incident Survey)
Hiroshi Suzuki (1.4.2 The Citadel Variant of ZeuS)
Yuji Suga (1.4.3 A Reflection on Issues Plaguing Protocols and Implementations Using Cryptographic Technology, and the Way Forward)
Office of Emergency Response and Clearinghouse for Security Information, Service Operation Division, IIJ

Yoshinobu Matsuzaki (1.4.1 An Overview of Tor)
Network Engineering Section, Network Service Department, IIJ

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

*111 CA/Browser Forum, "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.0, 22 Nov. 2011" (http://www.cabforum.org/Baseline_Requirements_V1.pdf).
*112 IETF DNS-based Authentication of Named Entities (DANE) Working Group (https://datatracker.ietf.org/wg/dane/).
*113 Convergence (http://convergence.io/details.html).