Smartphone Security

In this report we look at the issue of many public keys used with SSL/TLS and SSH sharing the same private key as other sites, discuss the state of security on smartphones, and examine debate surrounding the supply of information for dealing with targeted attacks.

1.1 Introduction

This report summarizes incidents to which IIJ responded, based on general information obtained by IIJ itself related to the stable operation of the Internet, information from observations of incidents, information acquired through our services, and information obtained from companies and organizations with which IIJ has cooperative relationships. This volume covers the period of time from July 1 through September 30, 2012. In this period there were a number of website alterations and DDoS attacks in Japan related to historical dates in the Pacific War, and territorial disputes including Takeshima and the Senkaku Islands. A series of smartphone applications that acquire user information fraudulently or unnecessarily were also discovered, and this is becoming a major issue. At the same time, problems have also been identified in certain smartphone OSes and models, increasing the potential for exploitation. Additionally, groups such as Anonymous continue to carry out hacktivism activities in Japan. 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 July 1 and September 30, 2012. Figure 1 shows the distribution of incidents handled during this period*1.

The Activities of Anonymous and Other Hacktivists

Attacks by hacktivists such as Anonymous continued during this period. DDoS attacks and information leaks occurred at government-related and company sites in a large number of countries stemming from a variety of incidents and causes.

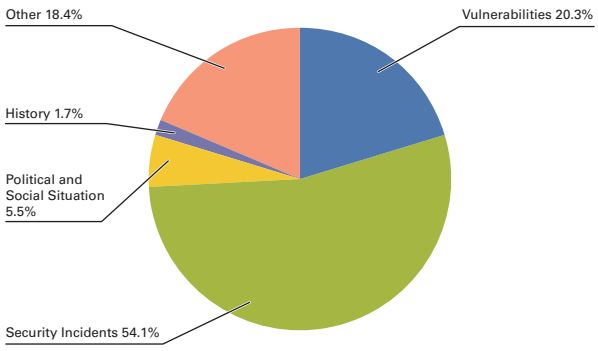


Figure 1: Incident Ratio by Category (July 1 to September 30, 2012)

In July, Anonymous altered multiple government websites in protest against moves by the Australian government to tighten Internet regulations. In a related incident, they also released a large amount of data obtained illegally from Australian ISPs and the Queensland state government (OpAustralia). In August, Anonymous launched attacks on multiple government websites in OpFreeAssange, which protested the English government's attempts to arrest WikiLeaks representative Julian Assange, who had been granted asylum by the Ecuadorian Embassy in London. In September, Anonymous launched OpTPB in retaliation for

*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.

the arrest of one of the co-founders of The Pirate Bay in Cambodia. This involved the alteration of a number of Cambodian government websites, as well as information leaks.

Additionally, ACTA (Anti-Counterfeiting Trade Agreement), which was rejected by the European Parliament in June after a heated protest campaign in European countries at the start of this year, was passed at the Japanese Lower House plenary session in September, paving the way for it to be signed into law. Japan is the first country to ratify the agreement. In response, anti-ACTA demonstrations also took place in some parts of Japan, but no notable attacks were observed.

■ Attacks Based on Political and Social Situation and Historical Context

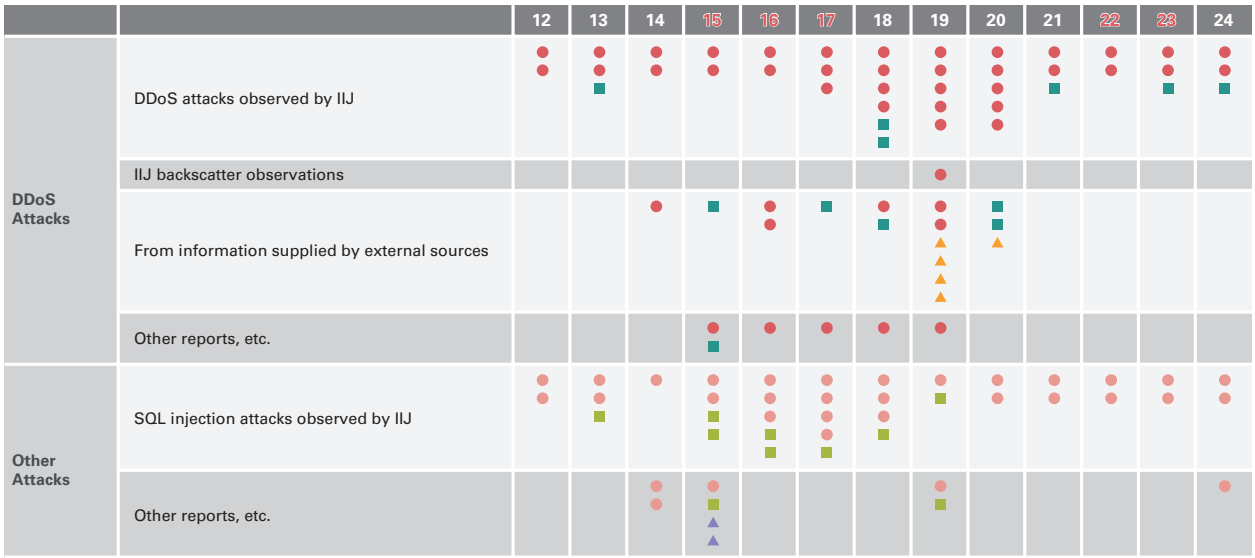
There were a number of international events during this period, such as the London Olympics held in July, and the APEC summit conference held in Russia in September. We remain vigilant due to attacks sometimes taking place on our networks when events such as these are held, but during this period no attacks related to these events were detected on IIJ facilities or client networks.

Meanwhile, during this period each year there are incidents related to historical dates in the Pacific War, and territorial disputes such as Takeshima and the Senkaku Islands. In this year in particular, there were a number of website alterations in Japan triggered by the illegal landing of Chinese activists on the Senkaku Islands in August.

There were also large-scale demonstrations in China and a series of major alterations and DDoS attacks on numerous websites for government agencies and private-sector businesses in Japan, in response to the nationalization of the Senkaku Islands by the Japanese government on September 11. Table 1 summarizes attacks determined to be related to these incidents based on information such as attack threats. One interesting aspect of the attacks this year is there were more victims of website alterations than in attacks last year. Less damage was caused by DDoS attacks. Attacks attempting to alter websites were not limited to government institutions, and were also made on financial institutions and general companies. It is believed these attacks were carried out using SQL injections and brute force attacks on web servers.

A number of government institutions and private-sector businesses were among the attack targets, but attacks observed by IIJ did not involve very many targets or incidents. At just after 10 PM on September 18 (Japan time), synchronized attacks on multiple targets were detected. The largest attacks observed on a single target were 650Mbps/240Kpps UDP and SYN floods. DDoS attack types included HTTP GET floods and connection floods, and many attacks on servers were observed. The largest DDoS attack observed during the current period was an 800Mbps/110Kpps compound attack. The longest sustained attack lasted for about one hour.

Table 1: Overview of Serial Attacks (September 2012)



We have tallied the attacks detected by IIJ during the current period that correspond to attack threats, and categorized them as either DDoS attacks or other attacks.
SQL injection attacks and website alterations targeting web servers fall into the "other" category.
Days in which attacks were made on specific servers are marked, with a single mark used even when multiple attacks were made on a server in the same day.
However, because DDoS attacks and other attacks are tallied separately, two marks may appear for a single server when it was targeted by DDoS attacks and website alterations at the same time.

- ● Government Agency-Related/ DDoS Attacks
- ● Government Agency-Related/ Other Attacks
- ▲ Educational Institution-Related/ DDoS Attacks
- ▲ Educational Institution-Related/ Other Attacks
- ■ General Companies and Organizations/ DDoS Attacks
- ■ General Companies and Organizations/ Other Attacks

July Incidents

1 **1st:** A leap second was inserted to adjust Coordinated Universal Time at 8:59:60 AM Japan time.
National Institute of Information Communications Technology (NICT), "Notification of 'leap second' insertion - July 1 will be one second longer this year -" (http://www.nict.go.jp/press/2012/01/31-1.html) (in Japanese).

2

3 **3rd:** Twitter published their first Transparency Report (a report summarizing the state of requests to disclose user information from government institutions in each country). This report covers the period between January and June 2012, and it shows that Japan was second behind the United States in the number of requests.
"Twitter Transparency Report" (https://support.twitter.com/articles/20170002).

4

5 **3rd:** Japan deposited the Instrument of Acceptance of the "Convention on Cybercrime". As a result it will come into effect from November 1 of this year.
Ministry of Foreign Affairs, "Convention on Cybercrime" (http://www.mofa.go.jp/announce/announce/2012/7/0704_01.html).

6 **4th:** The government's Information Security Policy Council was held, and the "Information Security 2012" annual plan was finalized, advocating stronger countermeasures for sophisticated attacks such as targeted attacks, and support for new telecommunications technologies such as smartphones and cloud computing.
National Information Security Center, "Information Security 2012" (http://www.nisc.go.jp/eng/pdf/is2012_eng.pdf).

7

8 **9th:** At 1:01 PM Japan time, the DNS server run by the FBI for those infected with DNS Changer ceased operation.
DCWG, which had been working on countermeasures for DNS Changer, made the following announcement. "DCWG Ends Clean DNS Function" (http://www.dcwg.org/dcwg-ends-clean-dns-function/).

9

10 **10th:** Microsoft published their Security Bulletin Summary for July 2012, and released three critical updates including MS12-043, as well as six important updates.
"Microsoft Security Bulletin Summary for July 2012" (http://technet.microsoft.com/en-us/security/bulletin/ms12-jul).

11

12 **12th:** The Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry founded a Cyber Attack Analysis Council together with four related organizations with the aim of grasping the state of cyber attacks and providing related ministries and agencies, and important infrastructure business operators with the results.
Ministry of Internal Affairs and Communications, "Cyber Attack Analysis Council to be Held" (http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000021.html) (in Japanese). A summary of proceedings at the 1st council can be found on the following Ministry of Economy, Trade and Industry website. Ministry of Economy, Trade and Industry, "Cyber Attack Analysis Council" (http://www.meti.go.jp/committee/kenkyukai/mono_info_service.html#cyber_attack) (in Japanese).

13

14

15 **13th:** Problems were caused when a domain registrar in Japan temporarily suspended DNS services to a user for a terms of service violation, affecting users of the services provided on the corresponding domain.

16 **17th:** The Information-technology Promotion Agency (IPA) published a report titled "Survey of Incidents Caused by the Fraudulent Activity of Organization Insiders," which outlines the current state and awareness of internal fraud.
"Survey of Incidents Caused by the Fraudulent Activity of Organization Insiders" Report Published (http://www.ipa.go.jp/security/fy23/reports/insider/index.html) (in Japanese).

17

18 **18th:** Oracle released their quarterly scheduled update for a number of products including Oracle, fixing a total of 87 vulnerabilities.
"Oracle Critical Patch Update Advisory - July 2012" (http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html).

19 **19th:** The C&C servers for the Grum Botnet, said to be the third largest in the world, were taken down, rendering it inactive.
Details were provided by The Spamhaus Project, which took part in the takedown. "Spam botnets: The fall of Grum and the rise of Festi" (http://www.spamhaus.org/news/article/685/spam-botnets-the-fall-of-grum-and-the-rise-of-festi).

20

21 **20th:** A vulnerability (CVE-2012-2978) in the NSD authoritative DNS server implementation that caused abnormal termination when specially-crafted DNS packets were received was discovered and fixed.
NLnet Labs, "NSD denial of service vulnerability from non-standard DNS packet from any host on the internet. [VU#624931 CVE-2012-2978]" (http://www.nlnetlabs.nl/downloads/CVE-2012-2978.txt).

22

23 **25th:** A vulnerability (CVE-2012-2808) that made DNS poisoning attacks possible due to problems with source port and TXID randomness in DNS implementations for Android versions earlier than 4.0.4 was discovered and fixed.
See the following IBM Application Security Insider for details. Android DNS Poisoning: Randomness gone bad (CVE-2012-2808) (http://blog.watchfire.com/wfblog/2012/07/android-dns-poisoning-randomness-gone-bad-cve-2012-2808.html).

24

25 **25th:** A vulnerability (CVE-2012-3817) in BIND 9.x that could cause a crash when large numbers of DNSSEC validations are received was discovered and fixed.
Internet Systems Consortium, "CVE-2012-3817: Heavy DNSSEC Validation Load Can Cause a 'Bad Cache' Assertion Failure in BIND9" (https://kb.isc.org/article/AA-00729).

26

27 **25th:** A vulnerability (CVE-2012-3868) in BIND 9.9.x that could cause a crash due to a memory leak when large numbers of TCP requests are received was discovered and fixed.
Internet Systems Consortium, "CVE-2012-3868: High TCP Query Load Can Trigger a Memory Leak in BIND 9" (https://kb.isc.org/article/AA-00730).

28

29 **29th:** At a security event held in the United States, a cloud service was announced that uses a known vulnerability in MS-CHAPv2, which is used for authenticating encrypted communications, to uncover authentication information quickly and at little cost.
See the discoverer's following blog post for more details. 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/).

30

31 **30th:** The Telecom Information Sharing and Analysis Center issued a warning regarding a vulnerability found in some Logitec brand wireless LAN broadband routers that was disclosed in May.
"[Warning] Logitec Brand Router Vulnerability, and Steps to be Taken by Users" (https://www.telecom-isac.jp/news/news20120730.html) (in Japanese).

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

*Dates are in Japan Standard Time

■ Attacks Exploiting Unpatched Vulnerabilities

During this period we confirmed a number of cases in which unpatched vulnerabilities were discovered and exploited. On August 26 it was reported that there was an unpatched vulnerability (CVE-2012-4681) in Oracle's Java 7 that allowed execution of arbitrary OS commands, and it had already been exploited*2. Because PoC (Proof of Concept) code had been published and a number of anti-virus vendors had already reported attacks exploiting this vulnerability*3, Oracle released an unscheduled patch for this vulnerability on August 31. This vulnerability only functions with the latest Java version 7, and does not affect the older Java version 6. On September 18, an unpatched vulnerability in Internet Explorer was reported*4. This vulnerability had already been exploited by the time it was disclosed, and Microsoft released a patch on September 22*5.

Attacks exploiting unpatched vulnerabilities such as these are a frequent occurrence, and affected devices are wide open to attacks until a patch is released. This means that users must take action themselves, such as implementing countermeasures recommended by vendors to reduce the impact. When an attack could have a profound effect, users may even need to temporarily suspend use of the software containing the vulnerability, or uninstall it and use alternative software.

■ Vulnerabilities and their Handling

During this period fixes were released for Microsoft's Windows*6*7, Office*8*9, and Internet Explorer*10. A security update (MS12-043) for a vulnerability in Microsoft XML Core Services that was released on July 11 was re-released in August to add support for Microsoft XML Core Services 5.0. Updates were also made to Adobe Systems' Adobe Reader and Acrobat, Adobe Flash Player, and Oracle's Java, fixing many vulnerabilities. Vulnerabilities in Apple's iOS were also fixed with the release of a new version.

A vulnerability that makes DNS poisoning possible in DNS resolver implementations was discovered and fixed in Android, which is used as the OS for mobile devices such as smartphones and tablets.

Regarding server applications, a quarterly update for the Oracle database server was released, fixing a number of vulnerabilities. A number of vulnerabilities in BIND DNS servers that could cause abnormal server termination through the use of specially crafted Resource Records were fixed. A vulnerability that could cause abnormal server termination was also discovered and fixed in the NSD authoritative DNS server implementation, which is also used in root servers.

*2 FireEye Malware Intelligence Lab, "ZERO-DAY SEASON IS NOT OVER YET" (http://blog.fireeye.com/research/2012/08/zero-day-season-is-not-over-yet.html).

*3 See the following Trend Micro SECURITY BLOG post for an explanation of the behavior of a malicious program that exploits this vulnerability. "Java Runtime Environment 1.7 Zero-Day Exploit Delivers Backdoor" (http://blog.trendmicro.com/trendlabs-security-intelligence/java-runtime-environment-1-7-zero-day-exploit-delivers-backdoor/).

*4 "Microsoft Security Advisory (2757760) Vulnerability in Internet Explorer Could Allow Remote Code Execution" (http://technet.microsoft.com/en-us/security/advisory/2757760).

*5 "Microsoft Security Bulletin MS12-063 - Critical: Cumulative Security Update for Internet Explorer (2744842)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-063).

*6 "Microsoft Security Bulletin MS12-043 - Critical: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2722479)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-043).

*7 "Microsoft Security Bulletin MS12-053 - Critical: Vulnerability in Remote Desktop Could Allow Remote Code Execution (2723135)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-053).

*8 "Microsoft Security Bulletin MS12-046 - Important: Vulnerability in Visual Basic for Applications Could Allow Remote Code Execution (2707960)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-046).

*9 "Microsoft Security Bulletin MS12-060 - Critical: Vulnerability in Windows Common Controls Could Allow Remote Code Execution (2720573)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-060).

*10 "Microsoft Security Bulletin MS12-052 - Critical: Cumulative Security Update for Internet Explorer (2722913)" (http://technet.microsoft.com/en-us/security/bulletin/ms12-052).

August Incidents

1 O **9th:** Oracle announced they were extending the end of support for Java 6 from November 2012 to February 2013.
"Java 6 End of Public Updates extended to February 2013" (https://blogs.oracle.com/henrik/entry/java_6_eol_h_h).

2 V **10th:** A presentation on the issue of many public keys used with SSL/TLS and SSH unintentionally sharing a private key with other sites was given at a security conference held in the United States.
3 See the following 21st USENIX Security Symposium presentation for more details. "Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices"
4 (https://www.usenix.org/conference/usenixsecurity12/mining-your-ps-and-qs-detection-widespread-weak-keys-embedded-devices).

5 P **10th:** The President of South Korea visited Takeshima.

6 V **15th:** Microsoft released an update that restricted the use of certificates using RSA keys less than 1024 bits in length, which lead to private keys having a high chance of being factored.
7 "Microsoft Security Advisory (2661254) Update For Minimum Certificate Key Length"
(http://technet.microsoft.com/en-us/security/advisory/2661254).

8 V **15th:** Microsoft published their Security Bulletin Summary for August 2012, and released five critical updates including MS12-060, as well as four important updates.
Security Bulletin Summary for August 2012" (http://technet.microsoft.com/en-us/security/bulletin/ms12-aug).

9 V **15th:** A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
10 "Security update available for Adobe Flash Player" (http://www.adobe.com/support/security/bulletins/apsb12-18.html).

11 V **15th:** A number of vulnerabilities in Adobe Reader and Acrobat that could allow unauthorized termination and arbitrary code execution were discovered and fixed.
"Security update available for Adobe Reader and Acrobat" (http://www.adobe.com/support/security/bulletins/apsb12-16.html).

12 P **15th:** An incident in which Chinese activists were arrested for landing on the Senkaku Islands illegally occurred.

13 S **15th:** AT&T DNS servers in two locations were targeted in DDoS attacks, affecting services provided to customers.

S **15th:** An attack was launched on a major bulletin board in Japan in relation to the anniversary of the end of World War II.

14

15 V **17th:** A vulnerability in Samsung and HTC Android mobile devices that allowed information entered by users to be referenced was discovered and fixed.
16 US-CERT "Vulnerability Note VU#251635 Samsung and HTC android phone information disclosure vulnerability"
(http://www.kb.cert.org/vuls/id/251635).

17 S **19th:** A number of websites in Japan were altered in relation to the arrest of Chinese activists who landed on the Senkaku Islands.

18 V **22nd:** Multiple vulnerabilities in Adobe Flash Player that could allow DoS attacks and arbitrary code execution were discovered and fixed.
19 "Security updates available for Adobe Flash Player" (http://www.adobe.com/support/security/bulletins/apsb12-19.html).

20 O **23rd:** The National Police Agency announced they had established a "Fraudulent Communications Prevention Council for Cyber Intelligence Countermeasures," to prevent incidents by working with security service providers and sharing information about cyber attacks thought to target information theft.
21 "Recent Developments in Cyber Intelligence (H1 2012)" (https://www.npa.go.jp/keibi/biki3/20120823kouhou.pdf) (in Japanese).

22 S **26th:** A man was arrested on charges of forcible obstruction of business for allegedly posting death threats on the website of a local public body. It was later revealed that the crime was committed by a third party via a virus infection, and the man was released.

23 V **27th:** It was announced that there was an unpatched vulnerability (CVE-2012-4681) in Oracle's Java 7 allowing execution of arbitrary OS commands that had already been exploited in attacks.
24 FireEye Malware Intelligence Lab, "ZERO-DAY SEASON IS NOT OVER YET"
(http://blog.fireeye.com/research/2012/08/zero-day-season-is-not-over-yet.html).

25

26 S **28th:** A former employee who had been dismissed from his contracting job was charged with fraudulently obtaining sensitive information from the U.S. subsidiary of a Japanese company that he worked for.
27 Sophos Naked Security Blog, "Toyota says it was hacked by ex-IT contractor, sensitive information stolen"
(http://nakedsecurity.sophos.com/2012/08/29/toyota-says-it-was-hacked-by-ex-it-contractor-sensitive-information-stolen/).

28 S **30th:** RIKEN issued a warning about targeted attack email sent in the guise of invitations to an event co-hosted by the Advanced Institute for Computational Science.
29 "A Warning Regarding Targeted Attack Email Misrepresented as From the Advanced Institute for Computational Science"
(http://www.riken.go.jp/r-world/topics/120830/index.html) (in Japanese).

30 V **31st:** Oracle released a fix for an unpatched vulnerability discovered in Java 7.
"Oracle Security Alert for CVE-2012-4681" (http://www.oracle.com/technetwork/topics/security/alert-cve-2012-4681-1835715.html).

31 P **31st:** The Anti-Counterfeiting Trade Agreement (ACTA) was approved by the Foreign Affairs Committee of Japan's House of Representatives.

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

*Dates are in Japan Standard Time

Dealing with the DNS Changer Malware

Regarding the DNS Changer malware*11, the interim DNS server run by the FBI ceased operations as scheduled on July 9 at 1:01 PM Japan time. However, no major disruptions were observed, in part due to extensive initiatives to warn the general public in Japan and other countries around the world.

According to a tally of unique IP addresses for infected PCs carried out by the DCWG (DNS Changer Working Group)*12, at its peak there were over 800,000 infections (November 16, 2011), but this number ultimately dropped to 210,000, or about a quarter of the peak level. As of July 8, according to data on the number of IP addresses by country, there were 5,522 infections in Japan.

The threat of DNS Changer lies not only in the number of infected users, but in the fact that it hijacks the DNS system essential for Internet use by changing DNS server settings on an infected PC. By redirecting infected users to malicious servers in this way, actual financial damages were caused through methods such as taking over ad traffic and distributing scareware. Regarding other incidents in which the technique of changing DNS server settings was used, there were also reports of attacks on home routers in Brazil*13. Because it is difficult for users and ISPs to notice when the DNS server referenced is changed in this way, similar techniques could be exploited again in the future.

The State of Smartphones and the Increase in Malware

During this period a vulnerability that made it possible to remotely reset some Samsung Android devices to their factory defaults was disclosed*14. A vulnerability in the Yahoo! app for Android devices was also exploited to hijack the email account used by the application and send spam*15. A glitch that made it possible to circumvent in-app billing was discovered in iOS*16. A vulnerability related to the WebView class was discovered and fixed in an HTML-based Android application SDK (software development kit) supplied by Japanese SNS providers. It caused information in the data area of applications utilizing the SDK to be leaked when other fraudulent Android applications were used.

The threat of viruses and malware is also on the rise. A suspicious Android application targeting Japanese users made news when it was discovered in April, and many applications thought to emulate it have also been identified during the current period. Many of these applications claim to resolve common sources of user dissatisfaction, by extending battery life or improving signal quality after installation, for example. As a result, the IPA issued a warning explaining an example behavior of a fraudulent application, based on analysis of applications such as these*17. Techniques used by these applications to redirect users include sending spam containing links to malicious sites to mobile devices, which make it difficult to confirm whether mail is legitimate. Social networking services have also been used. See “1.4.2 Safe Use of Smartphones” for more information about smartphone-related issues such as these.

*11 See “1.4.2 DNS Changer Malware” in IIR Vol.15 (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol15_EN.pdf) for more information about the DNS Changer malware.

*12 Detection sites for each country can be found on the following DCWG site. “How can you detect if your computer has been violated and infected with DNS Changer?” (http://www.dcwg.org/?page_id=381).

*13 Kaspersky Lab SECURELIST Blog, “Massive DNS poisoning attacks in Brazil” (http://www.securelist.com/en/blog/208193214/Massive_DNS_poisoning_attacks_in_Brazil).

*14 F-Secure Blog, “Samsung TouchWiz Devices Vulnerable to Mischief” (http://www.f-secure.com/weblog/archives/00002434.html).

*15 Trend Micro Malware Blog, “Yahoo! Android App Vulnerability May Allow Spamming” (http://blog.trendmicro.com/trendlabs-security-intelligence/yahoo-android-app-vulnerability-may-allow-spamming/).

*16 9to5mac, “Apple’s in-app purchasing process circumvented by Russian hacker” (http://9to5mac.com/2012/07/13/apples-in-app-purchasing-process-circumvented-by-russian-hacker/).

*17 See “Watch out for a smartphone application that steals information!” in IPA’s “Computer Virus/Unauthorized Computer Access Incident Report - August 2012 -” (http://www.ipa.go.jp/security/english/virus/press/201208/documents/summary1208.pdf).

September Incidents

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

S **5th:** 24,000 BTC (worth approximately $250,000) was stolen from a Bitcoin exchange site. It is thought their servers were compromised, and keys found and stolen from a backup saved to an unencrypted area of the hard disk.

O **5th:** IPA presented their computer virus and unauthorized computer access incident report for August 2012, and issued a warning about an increase in applications targeting smartphone users in Japan.
"Computer Virus/Unauthorized Computer Access Incident Report - August 2012 -"
(http://www.ipa.go.jp/security/english/virus/press/201208/documents/summary1208.pdf).

O **6th:** The Anti-Counterfeiting Trade Agreement (ACTA) was approved at the Lower House plenary session.

O **8th:** Google announced they were acquiring security service provider VirusTotal.
VirusTotal, "An update from VirusTotal" (http://blog.virustotal.com/2012/09/an-update-from-virustotal.html).

S **11th:** U.S. Domain registrar the Go Daddy Group experienced a service outage of several hours. Anonymous claimed responsibility for this incident, but the Go Daddy Group state it was due to an internal router failure.
"Go Daddy Site Outage Investigation Completed" (http://www.godaddy.com/newscenter/release-view.aspx?news_item_id=410).

S **11th:** A junior high-school student was charged on suspicion of supplying electromagnetic records of a computer virus for distributing a virus that displayed images on PC screens. This was the first time a minor had been charged with this crime.

V **13th:** A vulnerability (CVE-2012-4244) in BIND 9.x that could allow external parties to cause a crash was discovered and fixed.
Internet Systems Consortium, "CVE-2012-4244: A specially crafted Resource Record could cause named to terminate"
(https://kb.isc.org/article/AA-00778).

V **13th:** Microsoft published their Security Bulletin Summary for September 2012, and released two important updates.
"Microsoft Security Bulletin Summary for September 2012" (http://technet.microsoft.com/en-us/security/bulletin/ms12-sep).

S **14th:** Microsoft announced that a takedown of the Nitol botnet (Operation b70) had been carried out by their Digital Crimes Unit (DCU).
See the following blog post for details. "Microsoft Disrupts the Emerging Nitol Botnet Being Spread through an Unsecure Supply Chain"
(http://blogs.technet.com/b/microsoft_blog/archive/2012/09/13/microsoft-disrupts-the-emerging-nitol-botnet-being-spread-through-an-unsecure-supply-chain.aspx).

S **17th:** CloudFlare published an explanation of how to launch and stop a 65Gbps DDoS attack.
CloudFlare blog, "How to Launch a 65Gbps DDoS, and How to Stop One" (http://blog.cloudflare.com/65gbps-ddos-no-problem).

S **18th:** A number of alterations and DDoS attacks were carried out on web servers for Japanese government institutions and private-sector businesses on and around this day.

S **19th:** It was reported that a number of websites had been altered in relation to attacks on Japanese websites that occurred on September 18.
The National Police Agency published the following overview of the impact caused. "Regarding Cyber Attacks Believed to be Related to the Senkaku Islands Issue" (http://www.npa.go.jp/keibi/biki3/20120919kouhou.pdf) (in Japanese).

V **20th:** iOS 6 was released, and a number of vulnerabilities including those that allowed arbitrary code execution were fixed.
Apple, "About the security content of iOS 6" (http://support.apple.com/kb/HT5503).

V **22nd:** Microsoft published an update related to a number of vulnerabilities in Internet Explorer, including those that could allow arbitrary code execution through viewing a malicious website.
"Microsoft Security Bulletin MS12-063 - Critical: Cumulative Security Update for Internet Explorer (2744842)"
(http://technet.microsoft.com/en-us/security/bulletin/ms12-063).

V **22nd:** The new 'CRIME' attack against TLS/SSL was presented at a security conference held in Argentina.

V **26th:** A vulnerability in some Android device versions that could allow remote reset to factory defaults was disclosed.
See the following Sophos Naked Security Blog post for more details. "Are Android phones facing a remote-wipe hacking pandemic?"
(http://nakedsecurity.sophos.com/2012/09/26/are-android-phones-facing-a-remote-wipe-hacking-pandemic/).

S **26th:** A copy of phpMyAdmin 3.5.2.2 containing a Trojan horse was discovered and fixed on a SourceForge mirror site.
"phpMyAdmin corrupted copy on Korean mirror server" (http://sourceforge.net/blog/phpmyadmin-back-door/).

S **26th:** Log files including unencrypted user information were inadvertently published on an FTP server at IEEE, leaking the information of 100,000 users.
"IEEE Statement on Security Incident" (http://www.ieee.org/about/news/2012/25september_2_2012.html).

O **27th:** Due to concerns regarding secrecy of communications, the Ministry of Internal Affairs and Communications presented its views on a new advertisement service that utilizes results from the analysis of user mail content, which was announced by a portal provider.
"Regarding Yahoo! JAPAN's New Advertising Service" (http://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000122.html).

V **29th:** Due to the discovery that one of its code signing certificates was being exploited by malware, Adobe announced it would take measures to revoke the impacted certificate in October.
"Security certificate updates" (http://helpx.adobe.com/x-productkb/global/certificate-updates.html).

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

*Dates are in Japan Standard Time

Government Agency Initiatives

Regarding government agency initiatives, the Information Security Policy Council was held, and the "Information Security 2012" annual plan was finalized. This plan incorporates countermeasures for cyber attacks such as targeted attacks, and support for new telecommunications technologies such as smartphones and cloud computing. An Executive Meeting of the Council for Promotion of Information Security Measures was also held*18 in response to frequent cyber attacks such as website alterations and DDoS attacks on government institutions from mid-September. At this meeting, requests were made to review the information systems managed at each government ministry, and enhance systems for dealing with failures and accidents.

Additionally, the National Police Agency, the Ministry of Internal Affairs and Communications, and the Ministry of Economy, Trade and Industry have been working on educating Internet users through activities such as the establishment of a portal site that compiles information on information security for Internet users to reference*19. It is also important to collaborate with other countries across borders to counter threats to information security. In light of this, a decision was made to launch initiatives from October to promote international cooperation and popularize information security measures in Japan by holding events involving international collaboration with countries in Asia, Europe, and the United States, as well as providing information on information security measures*20. This "International Information Security Campaign" serves to complement "Information Security Month," which is held in February each year.

Issues Regarding Cryptographic Algorithms' Strength and Certificate Use

During this period there were a number of issues with the compromise of cryptographic algorithms and the use of certificates.

At a security event in the United States in July, a tool for decrypting the MS-CHAP v2 authentication information used to authenticate PPTP (Point-to-Point Tunneling Protocol) for corporate VPN connections was disclosed. This tool exploited issues with the strength of the cryptographic algorithm used in the MS-CHAP v2 protocol that had been identified in the past. Microsoft published an advisory about this issue recommending the use of other protocols such as L2TP or combined use with PEAP*21.

At another security conference held in the United States in August, issues with the fact that many public keys used with SSL/TLS and SSH unintentionally share private keys with other sites were presented. See "1.4.1 The Issue of Many Public Keys Used with SSL/TLS and SSH Sharing Private Keys with Other Sites" for more information regarding this issue.

Microsoft also released an update that blocked the use of cryptographic keys less than 1024 bits in length on August 15. This was implemented to deal with the issue of RSA keys less than 1024 bits, which it is recognized should only be used by those understanding the risks involved. This update initially required manual installation by users, but it was included in automatic updates from October 10.

In September it was announced that there had been reports of fraudulent use of a code signing certificate used in Windows versions of Adobe applications. On October 5, measures were taken to revoke the impacted certificate included in the corresponding software that was signed after July 11.

*18 National Information Security Center, "Regarding the Executive Meeting of the Council for Promotion of Information Security Measures" (http://www.nisc.go.jp/press/pdf/kanjikai_press.pdf) (in Japanese).

*19 "Security From Here!" (http://www.ipa.go.jp/security/kokokara/) (in Japanese).

*20 The Chief Cabinet Secretary issued the following message about these initiatives. "Further Popularizing Security Measures - The Launch of an International Information Security Campaign -" (http://www.kantei.go.jp/jp/tyokan/noda/20120928message.html) (in Japanese).

*21 "Microsoft Security Advisory (2743314) Unencapsulated MS-CHAP v2 Authentication Could Allow Information Disclosure" (http://technet.microsoft.com/en-us/security/advisory/2743314).

1.3 Incident Survey

1.3.1 DDoS Attacks

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

■ Direct Observations

Figure 2 shows the circumstances of DDoS attacks handled by the IIJ DDoS Defense Service between July 1 and September 30, 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*22, attacks on servers*23, 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 853 DDoS attacks. This averages to 9.27 attacks per day, indicating an increase in the average daily number of attacks compared to our prior report. Bandwidth capacity attacks accounted for 0.1% of all incidents, server attacks accounted for 86.5%, and compound attacks accounted for the remaining 13.4%.

During this period there were a number of incidents related to territorial disputes. IIJ also detected DDoS attacks thought to be linked to these incidents. For example, 89.2% of the 249 attacks detected between August 15 and August 31, and 85.0% of the 326 attacks detected between September 10 and September 21, targeted public institutions including government agencies.

The largest attack observed during the period under study was classified as a compound attack, and resulted in 800Mbps of bandwidth using up to 110,000pps packets. Of all attacks, 69.8% ended within 30 minutes of commencement, 29.3% lasted between 30 minutes and 24 hours, and 0.9% lasted over 24 hours. The longest sustained attack was a server attack that lasted for one day, three hours, and 10 minutes (27 hours and 10 minutes).

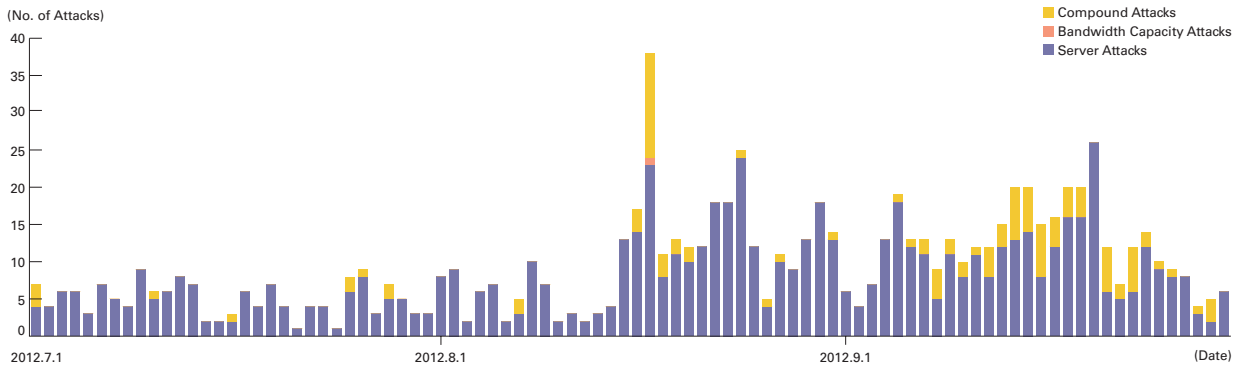


Figure 2: Trends in DDoS Attacks

*22 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.

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

In most cases, we observed an extremely large number of IP addresses, whether domestic or foreign. We believe this is accounted for by the use of IP spoofing*24 and botnet*25 usage as the method for conducting DDoS attacks.

Backscatter Observations

Next we present our observations of DDoS attack backscatter using the honeypots*26 set up by the MITF, a malware activity observation project operated by IIJ*27. By monitoring backscatter it is possible to detect some of the DDoS attacks occurring on external networks as a third party without any interposition.

For the backscatter observed between July 1 and September 30, 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 46.5% of the total during the target period. Attacks on ports such as 443/TCP used for HTTPS, 3389/TCP used for remote desktop, 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 China accounted for large proportions at 29.1% and 15.2%, 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 hosting provider in Hong Kong on July 26. A lot of backscatter was also observed from IP addresses in the United States and China on this day.

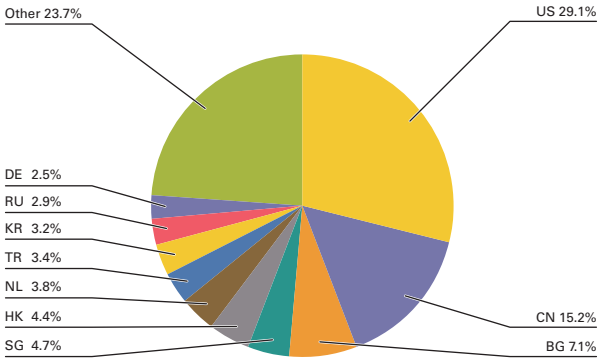


Figure 3: Distribution of DDoS Attack Targets According to Backscatter Observations (by Country, Entire Period under Study)

Backscatter from Hong Kong was also seen on August 14, and this was attributed to an anti-DDoS service provider in Hong Kong. Many attacks on Web servers (443/TCP) were observed on September 1, September 5, and September 7. These were linked to attacks on a number of servers for a hosting provider in Singapore. On September 23 attacks on Web servers for an anti-DDoS service provider in the United States were also observed, but these targeted a financial institution.

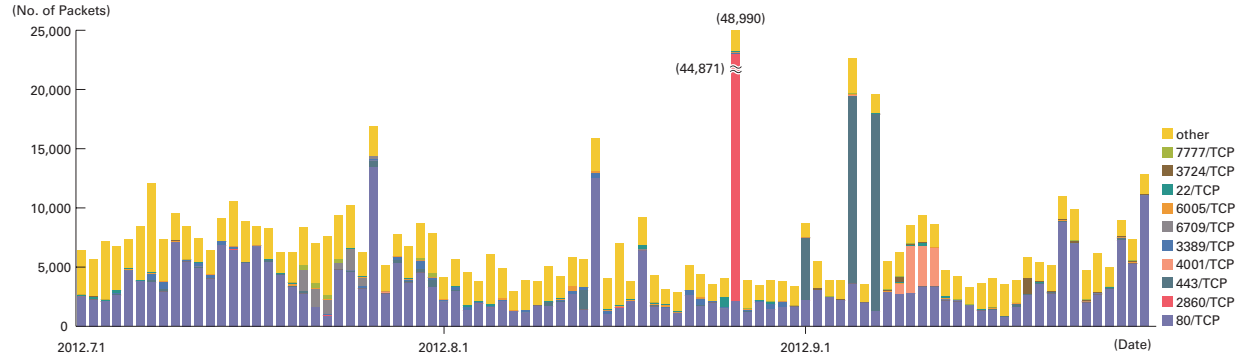


Figure 4: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)

*24 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.

*25 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."

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

*27 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).

On September 30, backscatter from a number of Web servers was observed, along with attacks on Web servers in the Philippines and the United States. These attacks targeted Web servers for the same bookmaker. On the same day attacks were also observed on the Web servers for an anti-DDoS service provider in Hong Kong and an adult site in Turkey.

On August 26, over 40,000 attacks on 2860/TCP targeting a server in Bulgaria were observed. Between September 9 and September 12, a total of more than 10,000 attacks on 4001/TCP targeting servers related to an online game in the United States were observed. These ports are not normally used by standard applications, so the purpose of the attacks is not known.

Notable DDoS attacks during the current survey period that were detected via IIJ's observations of backscatter included attacks thought have been carried out by TheWikiBoat on neo-Nazi sites in the United States in July, attacks by unknown perpetrators on Pastebin in September, and attacks believed to have been carried out by Anonymous on the Spanish police also in September.

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the MITF*28, a malware activity observation project operated by IIJ. The MITF uses honeypots*29 connected to the Internet in a manner similar to general users 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 June 1 and September 30, 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.

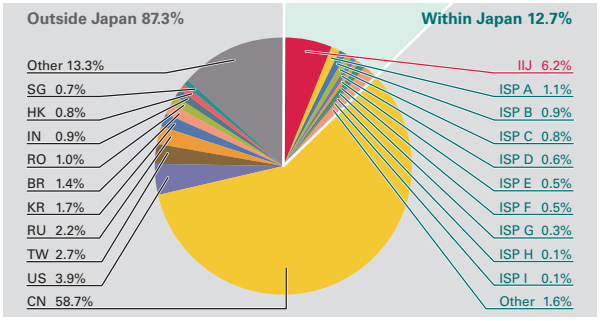


Figure 5: Sender Distribution (by Country, Entire Period under Study)

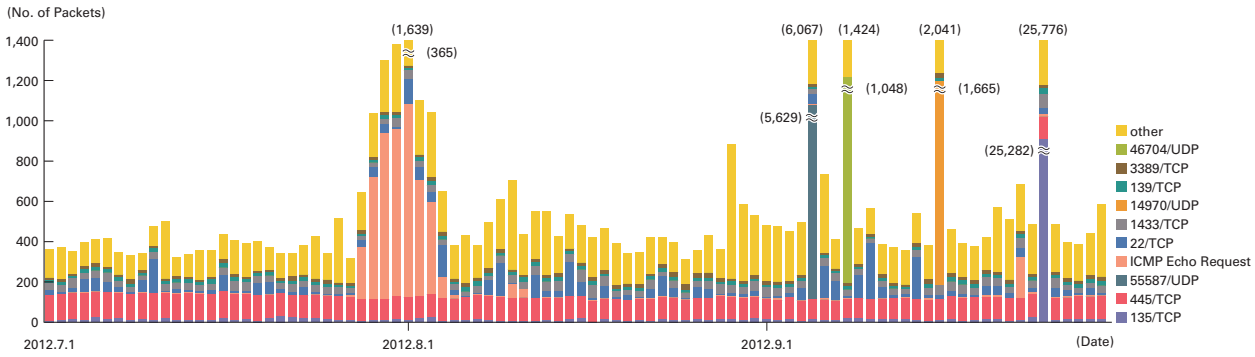


Figure 6: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

*28 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.

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

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 55587/UDP.

During this period, 135/TCP communications spiked on September 25. This was traced to high volumes of communications from a single IP address allocated to China. There was also a temporary rise in ICMP echo requests between July 28 and August 4. This involved communications from a single IIJ IP address to a specific honeypot. In addition to these, concentrated communications targeting 55587/UDP on September 5, 46704/UDP on September 8, and 14970/UDP on September 16 were received by a specific honeypot from multiple source IPs allocated to China, but their purpose is not known.

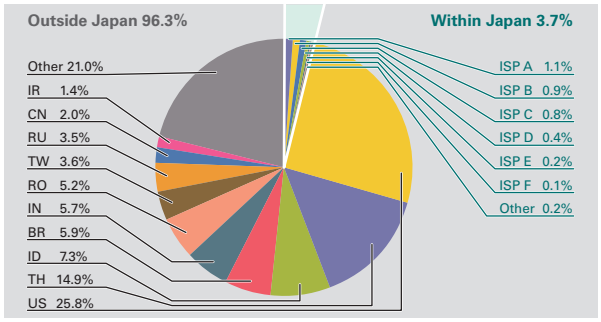


Figure 7: Distribution of Acquired Specimens by Source (by Country, Entire Period under Study, Excluding Conficker)

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 trends

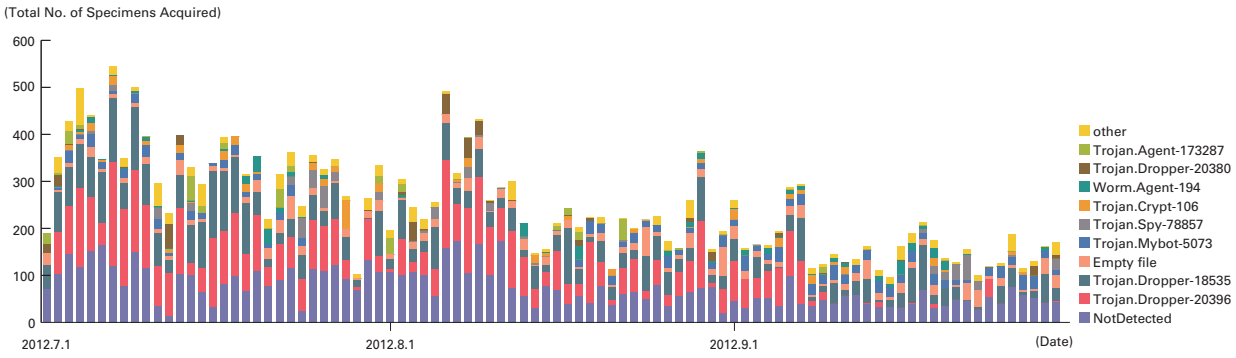


Figure 8: Trends in the Total Number of Malware Specimens Acquired (Excluding Conficker)

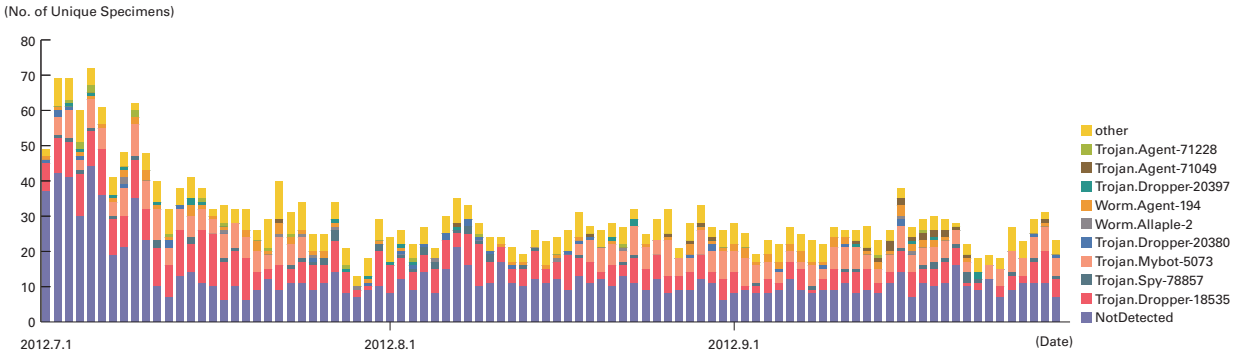


Figure 9: Trends in the Number of Unique Specimens (Excluding Conficker)

in the number of acquired specimens show the total number of specimens acquired per day*30, while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*31.

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, 249 specimens were acquired per day during the period under study, representing 31 different malware. Once again unknown specimens were acquired from Thailand and Indonesia, especially in July. After investigating these unknown specimens more closely, we learned that two types of bots*32*33 controlled by IRC servers had been active, as well as Trojan horse malware*34.

Under the MITF's independent analysis, during the current period under observation 81.4% of malware specimens acquired were worms, 13.8% were bots, and 4.8% were downloaders. In addition, the MITF confirmed the presence of 18 botnet C&C servers*35 and 10 malware distribution sites.

■ Conficker Activity

Including Conficker, an average of 46,415 specimens were acquired per day during the period covered by this report, representing 955 different malware. While figures rise and fall over short periods, Conficker accounts for 99.5% of the total number of specimens acquired, and 96.8% of unique specimens. This demonstrates that the Conficker worm remains the most prevalent malware by far, so we have omitted it from figures in this report. Although the total number of specimens acquired temporarily dropped by 13% in the previous survey period, for the current period this figure rose by 18%. In contrast, the number of unique specimens acquired dropped by about 3% compared to the previous report.

According to the observations of the Conficker Working Group*36, as of September 30, 2012, a total of 1,787,998 unique IP addresses are infected. This is a drop of approximately 44% compared to the 3.2 million PCs observed in November 2011, but it demonstrates that infections are still widespread.

*30 This indicates the malware acquired by honeypots.

*31 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.

*32 Trojan:Win32/Ircbrute (http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?name=Trojan%3AWin32%2FIrcbrute).

*33 Win32/Hamweq (http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fHamweq).

*34 Backdoor.Win32.Azbreg (http://www.securelist.com/en/descriptions/33537389/Backdoor.Win32.Azbreg.ccv).

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

*36 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*37. 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 June 1 and September 30, 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.

China was the source for 38.3% of attacks observed, while South Korea and Japan accounted for 22.9% and 21.9%, respectively, with other countries following in order. A greater number of SQL injection attacks against Web servers occurred compared to the previous report. Attacks from South Korea rose to second place, due to attacks from a specific attack source in South Korea directed at specific targets that occurred on certain days. Many attacks took place, with targets including public agencies, online games, and financial institutions.

During this period, attacks from a specific attack source in South Korea directed at specific targets took place on September 18. Attacks from a number of other attack sources each directed at specific targets also occurred on this day. On September 7 there were attacks from a specific attack source in China directed at specific targets. Attacks each from other specific attack sources directed at specific targets also took place on July 31 and August 22. These attacks are thought to have been attempts to find vulnerabilities on a Web server.

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

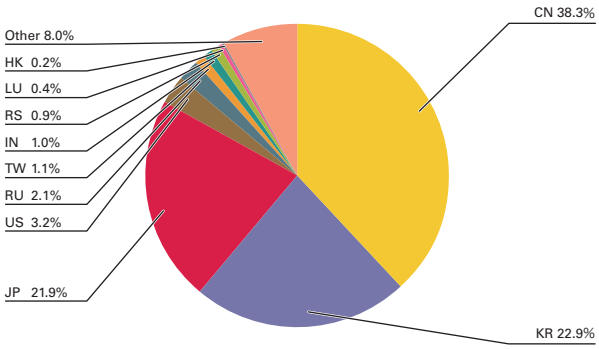


Figure 10: Distribution of SQL Injection Attacks by Source

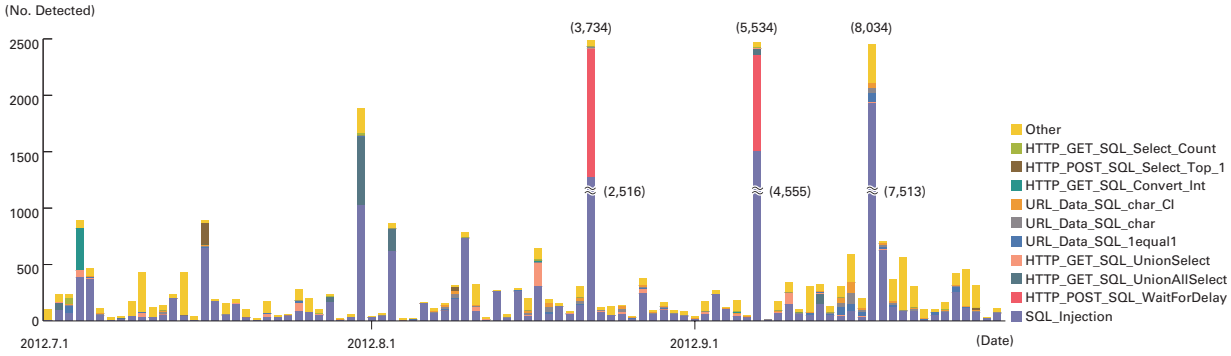


Figure 11: Trends in SQL Injection Attacks (by Day, by Attack Type)

*37 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 will present information from the surveys we have undertaken during this period, including discussion about the issue of many public keys used for SSL/TLS and SSH sharing a private key with other sites, a look at the state of smartphone security, and details of the debate about providing information for targeted attack countermeasures.

1.4.1 The Issue of Many Public Keys Used with SSL/TLS and SSH Sharing Private Keys with Other Sites

There have been reports from two independent groups, Lenstra et al.*38*39 and Heninger et al.*40, indicating 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. In this section we examine the state of this issue, look at its nature, and discuss ways to deal with it.

■ The Findings of the Heninger Group

Here we comment on the research paper presented by Heninger et al.*40 this year at the USENIX Security Symposium, where practical research presentations are given each year.

According to this research paper, 61% of 12.8 million SSL/TLS servers, and 65% of 10.2 million SSH servers, used the same private keys (repeated keys mentioned in) as other hosts. This is not necessarily a problem in all cases, as the same key is deliberately used for multiple IP addresses sometimes, such as when allocating multiple IP addresses to the same FQDN using techniques like round-robin DNS for load balancing. Of the IP addresses scanned, at least 5.93% (670,391 hosts) found were thought to be using the manufacturer default keys for SSL/TLS on devices. Most devices using the manufacturer default keys were network devices or embedded devices, and the authors are currently said to have contacted 60 vendors. A response of some kind was received from 20 of these, but as of now only three vendors have issued advisories*41. An advisory regarding a vulnerability using default keys on network devices has also been published separately from this research*42.

This research paper reports that upon collecting public key certificates and DSA signatures used with SSL/TLS and SSH via extensive scanning of 443/TCP (SSL/TLS) and 22/TCP (SSH) in the IPv4 address space on the Internet, 5.57% of SSL/TLS servers (714,243 IP addresses) and 9.60% of SSH servers (981,166 IP addresses) were unintentionally using the same public and private keys as other sites in an apparently vulnerable manner. Although it is not always a problem for different IP addresses to be using the same public and private keys, it has been warned that the same private key as a third party is unintentionally being used in some cases. In view of this situation, the authors began providing an online key-check service*43.

There have also been reports of default keys being used on other devices, such as Apache Web servers and Citrix remote access servers. Of these, 38 certificates were issued by certificate authorities trusted by Web browsers. Affected organizations include Fortune 500 companies, insurance companies, law firms, a major public transit authority, and the United States Navy., and the authors are said to be doing their best to notify these organizations.

*38 Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, Christophe Wachter, "Ron was wrong, Whit is right" (http://eprint.iacr.org/2012/064).

*39 Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, Christophe Wachter, "Public Keys" (http://www.iacr.org/conferences/crypto2012/abstracts/session11-2.html).

*40 Nadia Heninger, Zakir Durumeric, Eric Wustrow, J. Alex Halderman, "Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices" (https://www.usenix.org/conference/usenixsecurity12/mining-your-ps-and-qs-detection-widespread-weak-keys-embedded-devices).

*41 Summaries of this issue can be found in advisories from each vendor. "Security Advisories" (https://factorable.net/advisories.htm).

*42 "F5 BIG-IP remote root authentication bypass Vulnerability" (https://www.trustmatta.com/advisories/MATTA-2012-002.txt).

*43 You can check whether the public keys you are using are vulnerable or not on the following site. If you discover you are using vulnerable keys, it is recommended that you update them. "Widespread Weak Keys in Network Devices" (https://factorable.net/).

The research paper identifies issues with the pseudo-random number generator modules in wide circulation around the world as one of the factors causing this situation. It asserts that keys are not generated with enough key space due to insufficient entropy for the pseudo-random number generator modules used for generating keys and signatures, leading to the same private keys being shared.

The issues originating from a lack of entropy for pseudo-random number generator modules are already recognized, including as a Debian OpenSSL vulnerability*44. There was an issue with private keys being derived from a greatly reduced key space when generating keys using OpenSSL in certain versions of Debian. Although an advisory was issued in 2008, it has been reported that 0.03% of SSL/TLS servers (4,147 hosts) and 0.52% of SSH servers (53,141 hosts) still use these vulnerable keys. The authors also recommend a number of measures for each entity.

- **For device manufacturers**
  - Do not allow users to use built-in default keys or certificates.
  - Use hardware pseudo-random number generators to ensure sufficient entropy.
- **For end users**
  - Do not use default keys shipped with a device, or those generated during initial boot-up. Instead use keys generated in another environment that can ensure sufficient entropy.
  - Check whether keys you have generated are vulnerable, or in other words already being used by another user.
- **For certificate authorities**
  - Check whether public keys presented by customers are vulnerable, and do not issue certificates for vulnerable keys.

The Findings of the Lenstra Group

Here we present the findings of a research paper authored by Lenstra and others that was presented at CRYPTO 2012. The authors first collected 6,185,372 distinct X.509 certificates and 5,481,332 PGP public keys from a number of open public key certificate databases such as The EFF SSL Observatory*45. Below we detail the findings of this research paper regarding the RSA algorithm.

The report indicates that of 6,185,228 X.509 certificates including RSA public keys, 266,729 (4.3%) certificates included the same RSA public key as other certificates. Because in some cases these may be reused within the same organization, or in other words the same key pair used for both old and new certificates, these certificates are not all problematic. By clustering certificates that have the same key, they can be divided into 5,989,523 groups. Certificates in the same cluster mean that each has the same public key. 5,918,499 clusters (98.8%) contain a single certificate, or in other words a certificate in the cluster does not share a key with other certificates. The most highly populated cluster contained 16,489 certificates, and there were apparently 14 clusters with over 1,000 certificates.

Next the findings discuss the public keys for clustered certificates. A total of 6,386,984 distinct RSA public keys were obtained, consisting of 5,989,523 unique RSA public keys obtained from X.509 certificates, and RSA public keys acquired from PGP public keys in the same way. Looking into cases in which the same private key was shared, it was found that 12,934 public keys shared the same private keys. Of these, 36 public keys were matched with a combination of 9 different private keys. Heninger et al. also made the same observation, and problems have been identified when generating keys using a certain product.

*44 Debian Security Advisory, "DSA-1571-1 openssl -- predictable random number generator" (http://www.debian.org/security/2008/dsa-1571).

*45 Electronic Frontier Foundation, "The EFF SSL Observatory" (https://www.eff.org/observatory). This project collects a wide range of public key certificates used on HTTPS servers. The dataset is published to monitor whether there are problems with certificates issued by CA.

A System Allowing Third Parties to Identify Use of the Same Private Key

Some may question how a third party can identify that the same private keys are being used from the public key data collected. This is due to the following interesting property. While the fact that factoring of a large integer is difficult serves as the basis for the security of the RSA algorithm*46, it is also easy to find the GCD (greatest common divisor) of two different integers. The Euclidean algorithm that has been known since pre-Christian times is used to calculate the GCD. Normally, modular calculation of N=pq (the product of primes) is used for RSA, so it is difficult to find p or q from N, but easy to find q from $N_1=p_1q$ and $N_2=p_2q$. For this reason, as shown in Figure 12, it is possible to identify the prime q and p_1 and p_2 shared between Entity 1 with N_1 (and e_1) as its public key and Entity 2 with N_2 (and e_2) as its public key, revealing their private keys. Furthermore, it is also possible for third parties other than Entity 1 and Entity 2 to see that the same q is shared, so p_1, p_2, and q can all be identified by third parties.

As the above example demonstrates, the potential for a prime q supposedly selected at random to overlap by chance is a fundamental issue with the RSA algorithm. However, according to the prime number theorem*47, approximately $2^{1014.53}$ candidates for the 1024-bit primes used with 2048-bit RSA, indicating that it is not easy for them to overlap. That said, the algorithm can be biased when generating a prime randomly, or in other words issues are caused when a prime is not extracted from the entire $2^{1014.53}$ range. This means that the pseudo-random number generator module used to generate primes has a significant effect on the outcome.

The Impact of Shared Private Keys

When using the default keys for a device in the manner identified in these research papers, there is a higher chance that users with the same device will have the same private key. If you inadvertently share a private key with a third party, it could be exploited by those with the same private key, potentially leading to issues such as those shown in Table 2.

When using a key that could share a private key with a third party, we recommend that you change the key you are using to another key. You can check whether a public key is vulnerable or not using the online key-check service provided by the authors*41. As this demonstrates, it is important to be aware of the issue that vulnerable public keys can be identified by third parties, and that attackers can also obtain this information. If you may be affected, urgent measures are required.

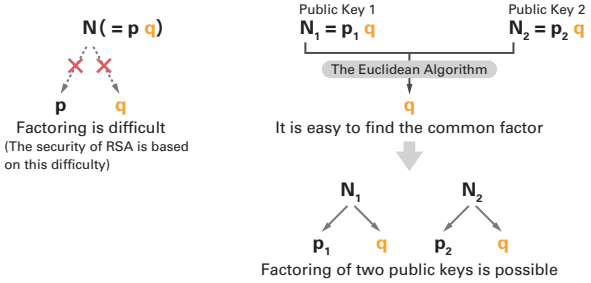


Figure 12: A System Allowing Third-Parties to Identify When Two Different Public Keys Share a Private Key.

Table 2: The Impact on Applications Using Public Key Cryptography when a Private Key is Leaked

Type of Impact	Details
1. Exposure of encrypted communications	The content of communications can be decrypted in environments capable of intercepting communications between SSL/TLS and SSH servers and clients, even when it is encrypted.
2. Server Spoofing	Environments capable of DNS spoofing or network hijacking can spoof SSL/TLS or SSH servers.
3. Unauthorized login or client spoofing	Login is possible using public key certificate, like mutual authentication for SSL/TLS.
4. Code signing of malicious programs	When the private key for a code signing public key certificate is leaked, it can be used to present programs as certified using this certificate.

*46 For example, with 2048-bit RSA, the 1024-bit length primes p and q are selected arbitrarily, and N=pq (2048-bit length) and e (normally 65537) disclosed as the public key. For the private key, d is calculated as ed=1 mod (p-1) (q-1). d can be calculated if p or q is known at this time (when the factoring of N is possible), while d is difficult to find when only N is known.

*47 The prime number theorem indicates an approximate value for the ratio of primes found in natural numbers, with the number of primes less than the integer n calculated as $\pi(n) \sim n/(\ln n + B)$, where B = -1.08366. Calculating the number of 1024-bit primes used with RSA2048 as $\pi(2^{1025}-1) - \pi(2^{1024}-1)$, we arrive at the figure of $2^{1014.53}$ (http://mathworld.wolfram.com/PrimeNumberTheorem.html).

1.4.2 Safe Use of Smartphones

Along with the popularization of smartphones, mobile phones have become more than just a means of communication, as they are now used for a variety of purposes, such as contacting friends via social networks, and downloading games and music for entertainment. Smartphones also feature network service device functionality approaching that of a PC. This has led to vulnerabilities and security issues that were previously unheard of in mobile phones. Here we discuss why incidents and issues occur on smartphones, and consider what should be done to use smartphones safely.

■ Incidents Related to Smartphones

There have already been many security incidents involving smartphones. These can be categorized into viruses, applications that fraudulently obtain information, the acquisition of information by legitimate applications, and information leaks from services linked to smartphones. We outline typical examples of each of these below.

■ Viruses

The first virus on an Android device was detected in August 2010*48. It was disguised as an application called Movie Player, but actually connected to a Short Message Service in Russia, and sent messages without authorization. Many viruses targeting smartphones run on Android devices, but viruses such as Ikee that run on iPhones have also been discovered*49. This means that the threat of viruses is present in all types of devices.

■ Applications that fraudulently obtain information

In April 2012 an application called "The Movie" that sent phone numbers and contact information on a device to a certain server became popular in Japan*50. IPA issued a warning about similar applications called "Denpa Kaizen" and "Denchi Nagamochi" in September 2012*51. These fraudulent applications send information unrelated to their operation to third parties. Because they use permissions authorized by the user during installation to send information, leaks occur regardless of whether or not there is a vulnerability.

■ Acquisition of information by legitimate applications

"Karelog" became a major topic of discussion in August 2011*52. Because location information and call logs for smartphones with this application installed could be checked from another computer, there were concerns about the leaking of private information.

■ Cloud service information leaks

In September 2011, it was revealed that the mail account used by American actress Scarlett Johansson had been compromised, and nude self-portrait photos she had taken and uploaded using her iPhone had been leaked. The perpetrator was later arrested by the FBI, and it was revealed he had accessed the accounts of over 50 other celebrities without authorization*53.

■ Reasons for the Increase in Smartphone Incidents

We believe the fact that smartphone-related incidents are on the rise can be attributed to smartphones having different characteristics to mobile phones and PCs. Here we take a closer look at the characteristics of smartphones.

■ Functional Characteristics of Smartphones

Smartphones are high-performance devices that feature GPS and camera functions and allow applications to be installed freely, in addition to basic call capabilities. The characteristics of smartphones differ from both mobile phones and PCs, creating new and unique problems.

---

*48 See the following Kaspersky Lab SECURELIST Blog post for more details. "First SMS Trojan for Android" (http://www.securelist.com/en/blog/2254/First_SMS_Trojan_for_Android).

*49 See the F-Secure Blog post, "First iPhone Worm Found" for details. (http://www.f-secure.com/weblog/archives/00001814.html).

*50 IPA issued a warning. "Computer Virus/Unauthorized Computer Access Incident Report - April 2012 -" (http://www.ipa.go.jp/security/english/virus/press/201204/documents/summary1204.pdf).

*51 IPA issued a warning. "Computer Virus/Unauthorized Computer Access Incident Report - August 2012 -" (http://www.ipa.go.jp/security/english/virus/press/201208/documents/summary1208.pdf).

*52 Karelog has now suspended its services. "Karelog" (http://karelog.jp/) (in Japanese).

*53 FBI press release, "Florida Man Arrested in 'Operation Hackerazzi' for Targeting Celebrities with Computer Intrusion, Wiretapping, and Identity Theft" (http://www.fbi.gov/losangeles/press-releases/2011/florida-man-arrested-in-operation-hackerazzi-for-targeting-celebrities-with-computer-intrusion-wiretapping-and-identity-theft).

- **The diversity of information on smartphones**
  A variety of information is uploaded and downloaded using smartphones, such as information from conventional contact and call log functions, as well as the photos, location information, videos, and text handled by applications. Smartphones are personal devices, and often contain a lot of personal information.
- **Elements that differ from PCs**
  Smartphone functions can be seen as similar to PCs from a user's point of view, but there are many differences from a security perspective, such as the technology used for security, methods for distributing software (applications), OS and application updates, the way that devices themselves are used, and communication methods.

Smartphone Service Architecture

In addition to smartphone functions, changes in the way business is provided are also believed to have introduced new problems. Conventional mobile phones featured a vertically-integrated business model for communication services, the development and supply of devices, and the supply of applications, with mobile phone carriers providing comprehensive services. However, smartphones feature horizontal business models, with each service supplied by a different provider to form a complete service package. This provides an open platform, but the division of responsibility for services becomes fragmented, making it more difficult to ensure overall platform security compared to vertically integrated models where it is easier to maintain consistency*54.

Security Model Issues

Permissions and sandboxing are the basic security models available for smartphones. These systems prevent applications from using functions they do not require access to. In Android, users can prevent unnecessary functions from being used by choosing whether or not to allow the permissions requested by applications when they are installed. The functions that an application uses are defined in categories such as access to the Internet or reference to contacts, and applications are not installed unless permission is given. However, this function has the following issues.

- Once permissions are allowed, they are not changed unless the application is uninstalled
- An application cannot be used unless all requested permissions are allowed
- Permission categories are tailored to OS functions and processing methods, so they are not intuitive for users (access to phone functions must be allowed to receive incoming calls while using an application, etc.)

Smartphones also feature a security function called a sandbox, which executes applications in an area isolated from the OS. However, unofficial applications that make it possible for general users to directly access OS functions outside sandbox constraints are available, and when these are used it is possible to bypass the sandbox security function. Additionally, unlike PCs, security software for smartphones is not given any special privileges, and runs in a sandbox like regular applications. As a result, it can sometimes be difficult to detect and defend against cases in which malware has targeted a vulnerability and obtained special privileges*55. For this reason, smartphones implementing their own security functions are also being developed*56.

Smartphone Applications

Smartphone applications are generally obtained from the official markets operated by Google, Apple, and mobile phone carriers, but there are also many unofficial markets that allow applications to be installed freely. Official markets each have their own methods for checking the security of applications*57, but unofficial markets may not check application security

*54 Mentioned in the Ministry of Internal Affairs and Communications' Final Report from the Smart Phone and Cloud Security Research Society (http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000020.html) (in Japanese) and Smartphone Privacy Initiative Proposal (http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000087.html) (in Japanese).

*55 The Fourteenforty Research Institute, Inc. has published detailed information. "Android: Technical Design Issues" (http://www.fourteenforty.jp/research/research_papers.htm) (in Japanese).

*56 Panasonic Corporation "Panasonic Develops New Solution to Protect Personal Data on Android™ Smartphones" (http://panasonic.co.jp/corp/news/official.data/data.dir/en120227-3/en120227-3.html).

*57 For example, Apple has published information about their app review for developers. "App Review Guidelines" (https://developer.apple.com/appstore/guidelines.html). Google uses a system called Bouncer to automatically check the security of applications. "Android and Security" (http://googlemobile.blogspot.jp/2012/02/android-and-security.html). Independent carrier measures include the security check used on KDDI CORPORATION's au one Market. "<Notice> Regarding Expanded Functionality for 'au one Market' <Attachment>" (http://www.kddi.com/corporate/news_release/2010/0831b/besshi.html) (in Japanese).

sufficiently, if at all. Because malicious applications have been distributed even on official markets in the past, there is also no assurance that official markets are 100% secure.

As mentioned in the anecdotal incidents, problems with the handling of user information have even been found in legitimate applications distributed on official markets, but there are currently no regulations regarding the handling of this kind of information. The Ministry of Internal Affairs and Communications' "Research Group for ICT Service Issues from a User's Perspective (FY 2009)*58" also looked into the handling of information related to user communications and location information in the hands of telecommunications carriers.

Furthermore, while user information used to be walled off within mobile phone carriers, with smartphones there is a chance that user information will be handled by platform providers such as Google and Apple and application developers, in addition to communications infrastructure providers. The Ministry of Internal Affairs and Communications is examining this issue in the "Research Group for ICT Service Issues from a User's Perspective" and the "Working Group regarding the Handling of User Information by Smartphones (FY 2011 to FY 2012 and ongoing)*59."

Wireless LAN

Another characteristic of smartphones is they support wireless LAN in addition to communications via mobile phone standards. Smartphones send and receive more data than conventional mobile phones, and mobile phone carriers actively promote the use of wireless LAN to free up communication bandwidth. Wireless LAN is very useful when connecting to the Internet in places difficult for a mobile phone signal to penetrate, such as inside buildings, but accidentally connecting to a malicious access point could lead to issues such as the interception of communications.

Network Services such as OS Updates and Backups

Like PCs, OS updates are also carried out for smartphones. However, fixes for vulnerabilities currently tend to be released more slowly than for PCs. Additionally, because individual users and application developers are responsible for OS and application updates and vulnerability fixes, as well as the encryption of backup data, users must stay aware of the relevant security information.

Furthermore, although backups should be proactively created from the perspective of availability, these cover a variety of smartphone data beyond personal information such as contacts and email, including applications and their data. This means that if backup data leaks, it causes damage equal to when the device itself is stolen.

Usage Situations

Because smartphones are multifunctional, feature high performance, have high resolution screens, are useful for more than just voice calls, and have superior portability, they are increasingly used in all manner of places. For this reason, the risk of snooping and theft is believed to be higher than regular mobile phones. These risks can be reduced using MDM (Mobile Device Management) if smartphone devices can be managed by an organization, but needless to say, individual users must use caution.

Precautions for the Safe Use of Smartphones

Currently, effort from both individual users and service providers is required to use smartphones safely. The Ministry of Internal Affairs and Communications is examining the issue from the perspective of both users and providers. Here we look at these initiatives, and discuss the kind of things that users should be aware of, as well as the steps that providers are likely to take in the future.

The "Smartphone Privacy Initiative" put together by the Ministry of Internal Affairs and Communications' "Research Group for ICT Service Issues from a User's Perspective," proposed comprehensive measures regarding smartphone privacy to allow users to use services securely and with peace of mind.

*58 Ministry of Internal Affairs and Communications, "Research Group for ICT Service Issues from a User's Perspective" (http://www.soumu.go.jp/menu_sosiki/kenkyu/11454.html) (in Japanese).

*59 Ministry of Internal Affairs and Communications, "Working Group regarding the Handling of User Information by Smartphones" (http://www.soumu.go.jp/menu_sosiki/kenkyu/riyousya_ict/02kiban08_03000087.html) (in Japanese).

1. Indicate a “smartphone user information handling policy” broadly applicable to smartphone-related providers that focuses on application providers and providers of data gathering modules, while also including operators of sites providing applications, OS providers, and mobile telecommunications carriers.
2. Propose measures for raising the effectiveness of policies, such as systems for third-party application validation.
3. Implement measures for supplying information and educating the public to improve user literacy.
4. Promote international collaboration.

The Smart Phone and Cloud Security Research Society also cited the following items for users as “Three Golden Rules for Smartphone Information Security.”

1. Update the OS (operating system)
2. Check the use of anti-virus software
3. Use caution when obtaining applications

Table 3 summarizes differences between PCs and smartphones, things users should be aware of, and areas for improvement, based on the characteristics of smartphones discussed here. Smartphones may appear at first glance to have simply become more convenient than conventional mobile phones, but because they feature methods for acquiring software and operating frameworks similar to PCs, a variety of security considerations are actually necessary. Important data such as personal information is often saved, sent and received on smartphones, but they are not yet as secure as PCs. It is important for users themselves to determine the importance of information, and consider whether this information should be placed on smartphones or related services, as well as whether a given application really needs to be used or not.

Smartphones appeared quite recently, and are still a developing platform. Security is expected to improve in the future through the efforts of providers and advances in technology, but even with more comprehensive technological countermeasures, the need for users to manage information will not go away, and nor will issues originating from the situations in which smartphones are used. There will be a continuing need for users to manage devices appropriately and use them safely. To this end, a sustained effort from both users and providers is required.

Table 3: Points to Note When Using Smartphones and Areas for Improvement

	PCs	Smartphones	Points for Users to Note	Areas for Improvement
OS	• Regarding urgent responses to vulnerabilities, updates appear in a timely manner • It is relatively rare for problems to appear in the OS when updates are made • Monthly automatic updates	• Slower response to vulnerabilities than PCs • Quality issues after updating the OS • User action is required to perform updates • There are issues such as jailbreaking and rooting	• Update the OS • Use devices that take security into account	When OS specifications are closely-managed by platform providers, this depends on the efforts of the platform provider. For open OSes, device manufacturers sometimes take their own measures
Applications	• Anti-virus software operates with higher privileges • Major applications are updated automatically • It is relatively easy to evaluate the security of applications	• Anti-virus software operates with the same privileges as general users • Updates are left up to application developers and users • Unofficial markets and unofficial applications exist, making it difficult to verify security	• Check the use of anti-virus software • Use caution when obtaining applications • Check the data accessed by applications • Check the reputation of the applications you are using • If an application acquires information it does not need, stop using it • Check the reputation of the network services you are using	Official market checks and independent security verifications by carriers are steadily improving
User Information	• There is little connection between user information and applications • Users can elect to take protective measures themselves	• Applications and user information are closely tied • Privileges used for applications lack granularity, and are not changed after they are granted	• Turn off functions that attach personal data such as GPS information when they are not required • Handle the authentication information for network services you use with care • Encrypt the backups you create as well as data uploaded to network services	Regulatory agency research societies and industry groups are examining better methods for handling user information
Wireless LAN	• A connection must be made intentionally	• Devices automatically connect to access points unintentionally in some cases, due to functions provided by carriers • It is hard/impossible to identify the access point	• Pay attention to the access point when using wireless LAN • Encrypt communications when using wireless LAN	The Ministry of Internal Affairs and Communications' Smart Phone and Cloud Security Research Society have raised issues, and these will be subject to future investigation
Device Management and Status of Use	• The locations and situations in which they are used are generally limited. Security wire and other solutions can be used when the location is physically fixed	• They are used in a diverse range of locations and situations, and are highly portable • They are used in the same manner as mobile phones	• Pay attention to your surroundings when using devices. As appropriate, determine whether or not it is an acceptable situation to work in • Do not use in public places where snooping could occur • Take measures to prevent theft or loss. In particular, do not place on tables in cafes, etc.	With regarding the corporate use, it is possible to limit damages using systems such as MDM. Conventional measures such as privacy filters are also effective

1.4.3 Sharing Information for Targeted Attack Countermeasures

Since the targeted attacks on major Japanese companies in August last year, a number of endeavors have been undertaken to deal with them, and a variety of countermeasures evaluated and implemented. Here we discuss the difficulty of sharing information about targeted attacks as a part of these endeavors, and examine ways to deal with this.

■ A Framework for Targeted Attack Countermeasures

To deal with the targeted attacks that came to light in rapid succession last year*60, activities have been undertaken from a variety of perspectives. For example, this issue has been addressed by the National Information Security Center's Information Security Policy Council*61, and a number of measures have been implemented by various ministries and agencies*62. The Information Security Operation provider Group Japan (ISOG-J) WG5*63, consisting of security-related companies in the private sector, is also tackling the issue.

Now, over a year since these efforts began, there have also been moves for even closer coordination between each activity*64.

IIJ participates in almost all of these activities, either directly or indirectly, because as a company responsible for critical communications infrastructure we could conceivably be subject to targeted attacks. We also consider it important to protect clients from targeted attacks via our security-related services.

Each of these activities focuses on reporting the detection of targeted attacks, and spreading this information broadly so it can be put to use in countermeasures.

Considering the potential for attacks of a scale where a nation or a specific industry is targeted, it is crucially important to gather information to get the entire picture. Research into a number of past incidents has shown that attack techniques are reused in many cases. This indicates that information sharing is necessary for implementing targeted attack countermeasures.

■ The Difficulty of Sharing Information About Targeted Attacks

To share information, that information must first be provided, but targeted attacks involve factors not found in typical cyber attacks that obstruct the sharing of information.

For example, the mail exploited in targeted attacks sometimes contains secrets regarding the attributes of the attack target (manager or researcher, etc.) or the company's line of business (defense-related industries, critical infrastructure). Information about the malware or vulnerabilities used in successful attacks may also be seen as revealing weaknesses in that company or IT system. To provide this information and share it with a large number of organizations and people involves significant risk for the information provider, and victims may be reluctant to provide information unless attacks were successfully defended.

Additionally, telecommunications carriers, security service providers, and system integrators are required to protect the secrets of customers based on information management regulations in related laws such as the Telecommunications Business Act, as well as non-disclosure clauses in individual agreements. Although these should of course be implemented

*60 See IIR Vol.14 "Targeted Attacks and Their Handling" (http://www.iij.ad.jp/en/company/development/iir/014.html) for an explanation of targeted attacks as well as specific incidents.

*61 The results of these discussions have been published under "Strengthening of Public-Private Sector Partnerships for Targeted Attacks" in the Information Security Policy Council's "Information Security 2012" annual plan (http://www.nisc.go.jp/eng/pdf/is2012_eng.pdf).

*62 Network for Sharing Cyber Intelligence Information (http://www.npa.go.jp/keibi/biki3/230804shiryou.pdf) (in Japanese), Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP) (http://www.ipa.go.jp/security/J-CSIP/index.html) (in Japanese), Telecom-ISAC Public-Private Council, National Information Security Center (NISC), CETPOART Council (http://www.nisc.go.jp/conference/seisaku/ciip/dai12/pdf/12siryou04.pdf) (in Japanese), etc.

*63 Information Security Operation providers Group Japan, WG5 Targeted Attack Countermeasure Evaluation WG (http://www.jnsa.org/isog-j/activities/index.html) (in Japanese).

*64 For example, the "Cyber Attack Analysis Council" (http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/120711_05.html) organized by J-CSIP and the Telecom-ISAC Public-Private Council, which is made up of organizations playing a leadership role, and the "Fraudulent Communications Prevention Council for Cyber Intelligence Countermeasures" (https://www.npa.go.jp/keibi/biki3/20120823kouhou.pdf) formed by the National Police Agency and ISOG-J, etc.

to ensure providers protect their customers, this is another reason why providers who have detected targeted attacks have been unable to share information externally*65.

Openly disclosing the fact that targeted attack detection and countermeasures are being implemented also has the side effect of informing attackers of the target's ability to detect and defend against attacks. For targeted attacks, it is assumed that the attacker has a strong sense of purpose, for example a desire to obtain specific information about a specific company. This means that when the attacker knows an attack has been detected and dealt with, they are likely to stop using the detectable technique, and launch attacks using another more sophisticated method.

As this demonstrates, if mistakes are made with regard to the scope of disclosure for information about targeted attacks, or the handling of the organization supplied with information, the organization that provided the information may be exposed to further risk. Information must be handled with sufficient care, and to that end a number of the countermeasure efforts introduced above cope with the issue by placing strict confidentiality obligations upon organizations provided with information.

■ Evaluating Information Sharing for Targeted Attack Countermeasures

Let us consider the kinds of information that organizations provided with information require. Here, we use the findings of Information Security Operation providers Group Japan (ISOG-J) WG5*66 as an example, and provide an account of its deliberations.

ISOG-J is a group consisting of Japanese security service providers, with each member providing security services to clients in some form. Working group activities are therefore carried out with the aim of preventing targeted attacks from succeeding using the services provided by each member. Three information sharing proof-of-concept tests related to targeted attacks were carried out by this working group last year, to evaluate what kinds of information would actually be useful for member countermeasure activities. Once information was acquired based on a number of conditions, members evaluated the data with a focus on how precisely and quickly countermeasures could be implemented on their service.

For the first test, assuming that "all information about a targeted attack was obtained," a mail attachment-based malware with a structure similar to the targeted attack was selected, and actual mail headers, address, body text, and malware information shared. For the second test, information on the name of malware specimens known to have been used in a targeted attack was shared. For the third test, information was shared regarding communications used in targeted attacks, such as the source of the mail, servers related to the download of the malware, and servers used to control the malware.

The results of these tests showed that when "all information was obtained", it took time to analyze the mail headers and malware, preventing swift measures being taken in some cases. It was also shown that malware specimen names were not standardized, due to differences in the anti-virus software used by each company, or in the timing of naming, making this information less than ideal for implementing countermeasures. The working group found that among security service providers, communication-related information was the easiest to handle and respond to.

This demonstrates that comprehensive information is not always required when sharing information for the purpose of security measures, and it can be said that there is an appropriate scope for information depending on the role it will play in countermeasures*67.

■ Information Sharing Success Cases

Here we will discuss information sharing success cases, using using the vulnerability information handling framework in Japan as an example. If someone who discovers a vulnerability in a product handles this information inappropriately, it can sour their relationship with the product developer, and they may be suspected of involvement in incidents that exploit this vulnerability. In Japan, the handling of this information can be entrusted to the Information Security Early Warning Partnership*68.

*65 In light of these circumstances, there have been moves to begin evaluating agreement templates that contain clauses regarding information sharing. National Information Security Center, "Information Security Policy Council Reference Material" (http://www.nisc.go.jp/conference/seisaku/) (in Japanese).

*66 Network Security Forum 2012 "Targeted Attacks and Security Operations" (http://www.jnsa.org/seminar/nsf/2012/data/B2_isog-j.pdf) (in Japanese).

*67 Based on these results, ISOG-J WG5 is continuing case studies with a focus on extracting information that makes it easier for providers to implement countermeasures.

*68 See IIR Vol.8 "Trends in Vulnerability Information Circulation" (http://www.iij.ad.jp/en/company/development/iir/008.html) for more information about the handling of vulnerability information, including the Information Security Early Warning Partnership.

The measures carried out uniformly under this framework include protecting discoverers by providing anonymity, consolidating vulnerability and product developer information through the IPA and JPCERT/CC and assigning corresponding responsibilities, and limiting the scope of information shared to promote countermeasures by only providing vulnerability information to product developers registered in advance. It also covers controlling the timing of the release of information to allow for the development of versions that fix vulnerabilities, and the release of information about patched products. This successfully eliminates risks for the discoverer of vulnerabilities, prevents the leak of vulnerability information before it is fixed, grants product developers more time to make fixes, and communicates information about patched products to users promptly.

■ Considering the Sharing of Information Regarding Targeted Attacks

As in this example, information about targeted attacks must be shared, so that similar attacks can be fended off by making the attack techniques (mail, vulnerabilities, or malware) and intentions of the attacker known, while protecting the secrets of the organization exposed to the attack. As we have discussed here, this requires the following:

- Consolidation of information by a responsible organization
- Protection of the targeted organization's information
- Analysis and extraction of information about the corresponding targeted attack
- Appropriate and swift supply of information to organizations with the ability to implement countermeasures
- Coordinated timing of announcements regarding attacks

The information sharing projects introduced earlier are also starting to implement information sharing that takes these points into account.

■ Summary

Many organizations that could be subject to targeted attacks are already participating in some form of information sharing, to bolster their own countermeasures by receiving information about attacks that have taken place at other organizations. Meanwhile, for information sharing activities to succeed, information must be provided by organizations that have been exposed to targeted attacks. By confirming how the items discussed here are being implemented and proactively sharing information, the activities your organization takes part in can help stimulate information sharing as a whole.

1.5 Conclusion

This report has provided a summary of security incidents to which IIJ has responded. In this report we discussed issues with the public keys available on the Internet, smartphone security, and debate regarding the sharing of information for targeted attack countermeasures. By identifying and publicizing incidents and associated responses in reports such as this, IIJ will continue to inform the public about the dangers of Internet usage, providing the necessary countermeasures to allow the safe and secure use of the Internet.

Authors:

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

Hirohide Tsuchiya (1.2 Incident Summary)
Hirohide Tsuchiya, Hiroshi Suzuki (1.3 Incident Survey)
Yuji Suga (1.4.1 The Issue of Many Public Keys Used with SSL/TLS and SSH Sharing Private Keys with Other Sites)
Masahiko Kato (1.4.2 Safe Use of Smartphones)
Mamoru Saito (1.4.3 Sharing Information for Targeted Attack Countermeasures)
Office of Emergency Response and Clearinghouse for Security Information, Service Operation Division, IIJ

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