IIR

Internet
Infrastructure
Review

Jun.2016
Vol.31

Infrastructure Security

Various Ransomware and Their Countermeasures

Messaging Technology

The Latest Trends in Spam

Technology Trends

TLS Trends

IIJ
Internet Initiative Japan

Internet Infrastructure Review

June 2016 Vol.31

Executive Summary

Recently there have been a lot of articles regarding the blockchains used as a core technology in virtual currencies. Although along with cryptographic technology these are expected to expand the potential for new business and technologies, we sense a certain amount of trepidation toward the use of increasingly complex and advanced technology, with Bitcoin among the methods used for the payment of ransom money resulting from ransomware. We have repeatedly covered technological trends for the safe and secure use of the Internet, and we believe it is our mission to dispel these fears by providing technological information that cultivates a better understanding of not just Internet infrastructure, but also security as it applies to the use of the Internet as social infrastructure.

This report discusses the results of the various ongoing surveys and analysis activities that IIJ, as a service provider, carries out to support the Internet and cloud infrastructure, and enable our customers to continue to use them safely and securely. We also regularly present summaries of technological development as well as important technical information.

In Chapter 1, we trace and analyze attacks and occurrences we have covered in the past, with a focus on incidents and events that took place day-to-day during the current survey period. As before, DDoS attacks by groups such as Anonymous continue to occur, and stemming from sites associated with the whaling controversy, attacks targeting public agencies and personal websites that do not seem directly related have also been observed. By discussing the current state of the growing damage caused by ransomware infections that employ increasingly sophisticated techniques to demand ransom money, and detailing countermeasures, we hope to provide some assistance for dealing with the situation. We also take a look at trends in international standardization regarding cryptography.

In Chapter 2, we examine messaging technology for the first time in about a year. Although there are temporary increases in the volume of spam, over the past few years there has been a general downward trend. Regarding technological trends, we discuss the features of DMARC in detail, while also giving a supplementary explanation based on information obtained from IIJ services.

In Chapter 3, we cover technological trends by going over the discussion of TLS at the IETF. The similar SSL technology was used for a long time, but from 2011 it was recommended that its use be prohibited, and that systems transition to TLS. However, it has been around 17 years since TLS was established, and eight years have already passed since the currently mainstream TLS 1.2 was drawn up, so work on developing TLS 1.3 is proceeding at a rapid pace. In this chapter, we hope to provide more insight by giving an explanation of operation using TLS 1.2, while also discussing the new technology to be incorporated in TLS 1.3, although it may ultimately change.

Around the time that this volume is published, the G7 Ise-Shima Summit will have finished, and the entire world will be waiting in anticipation for the Rio de Janeiro Olympic and Paralympic Games. I am sure that work toward bolstering social infrastructure and security measures will be happening at a breakneck pace behind the scenes. These days we have a stronger sense of the need to implement a range of security measures, and I hope that the articles in this report proved useful not only on the infrastructure side, but also for collaborating with users to consider efforts to protect the social infrastructure that the Internet has become.

Through activities such as these, IIJ continues to strive towards improving and developing our services on a daily basis, while maintaining the stability of the Internet. We will keep providing a variety of services and solutions that our customers can take full advantage of as infrastructure for their corporate activities.

Yoshikazu Yamai

Mr. Yamai is an Executive Managing Officer of IIJ and Director of the Service Infrastructure Division.
Upon joining IIJ in June 1999, he was temporarily transferred to Crosswave Communications, Inc., where he was engaged in WDM and SONET network construction, wide-area LAN service planning, and data center construction, before returning to his post in June 2004. After his return he was in charge of IIJ's Service Operation Division. From April 2016 he joined the Infrastructure Operation Division, and now oversees the overall operation of corporate IT services at IIJ. He also heads IIJ's data center operations, and he played a key role in the establishment of the modular "Matsue Data Center Park," which was the first in Japan to use outside-air cooling.

Various Ransomware and Their Countermeasures

1.1 Introduction

This report is a summary of incidents that IIJ responded to, based on information obtained by IIJ for the purpose of operating a stable Internet, information obtained from observed incidents, information obtained through our services, and information obtained from companies and organizations that IIJ has cooperative relationships with. This volume covers the period of time from January 1 through March 31, 2016. In this period a number of hacktivism-based attacks were once again carried out by Anonymous and other groups. A large number of DDoS attacks occurred, along with information leaks and website defacements. Attack operations targeting Japan have continued, with DDoS attacks targeting various websites including those of government agencies. There has been a rapid increase in damages caused by ransomware infections in Japan and overseas. For example, a case where a hospital in the United States paid a ransom has been reported. Also, there have been continuous unauthorized access attempts resulting in monetary damages through unauthorized use of loyalty points. These attacks seem to use lists of IDs and passwords obtained from another site. As shown here, many security-related incidents continue to occur across the Internet.

1.2 Incident Summary

Here, we discuss incidents handled and responded to by IIJ, between January 1 and March 31, 2016. Figure 1 shows the distribution of incidents handled during this period*1.

■ Activities of Anonymous and Other Hacktivist Groups

Attack activities by hacktivists such as Anonymous continued during this period. In correspondence with various events and assertions, DDoS attacks and information leaks targeted various companies and government-related sites.

As a protest against the drive hunting of dolphins and small whales in Japan, there have been intermittent DDoS attacks since last September which are believed to be performed by Anonymous. Various domestic sites have been affected by similar damages during this time period as well (OpKillingBay/OpWhales). In addition to targeting sites directly related to these activities, such as the website of the town of Taiji in Wakayama Prefecture, the official website of a documentary about the whaling controversy, and the website of an aquarium, other websites such as public agencies, airport companies, the personal website of the prime minister and other sites that had been attacked in the past have been continuously attacked. The attackers thought to be carrying out this operation have published multiple lists of attack targets, but many unlisted websites deemed to have no direct connection to the protests have also been affected. Although the attacks seemed to have slowed down a little since late March, caution is still required.

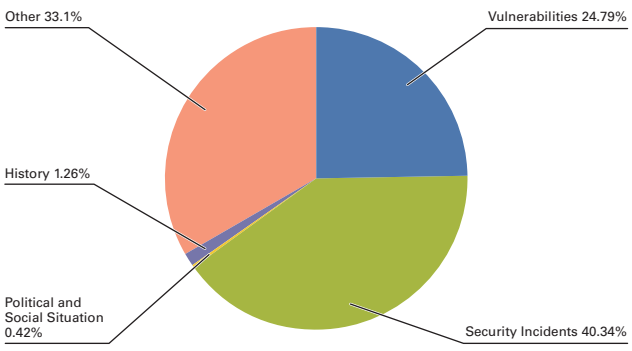


Figure 1: Incident Ratio by Category (January 1 to March 31, 2016)

In the Philippines, the website of the Commission on Elections (COMELEC) was attacked by the Anonymous Philippines and LulzSec Philippines groups in late March. The website was not only defaced, a database that contained the personal information of approximately 55 million Filipino voters was

*1 Incidents in this report are split into five categories: vulnerabilities, political and social situations, history, security incidents or other.
Vulnerabilities: Responses to vulnerabilities in network equipment, server equipment or software commonly used across the Internet or in user environments.
Political and Social Situations: Responses to attacks stemming from international conferences attended by VIPs and international conflicts, and other related domestic and foreign circumstances and international events.
History: Warnings/alarms, detection and response to incidents for attacks that occur on the day of a historically significant date that have a close connection to a past event.
Security Incidents: Unexpected incidents and related responses such as wide spreading of network worms and other malware; DDoS attacks against certain websites.
Other: Security-related information, and incidents not directly associated with security problems, including high traffic volume associated with a notable event.

stolen and made available on the Internet. The database included details such as passport-related data and fingerprint information, and there are concerns that this information may be exploited in the future.

■ Vulnerabilities and Responses

During this period many fixes were released for Microsoft's Windows[*2][*3][*4][*5][*6][*7][*8], Internet Explorer[*9][*10][*11], Office[*12][*13], and Edge[*14][*15][*16]. Updates were also released for Adobe Systems' Flash Player, Acrobat, and Reader.
A quarterly update was provided for Oracle's Java SE, fixing many vulnerabilities. Several of these vulnerabilities were exploited in the wild before patches were released.

In server applications, a quarterly update was released by Oracle, fixing many vulnerabilities in the Oracle database server and many other Oracle products. Multiple vulnerabilities were also discovered and fixed in the BIND9 DNS server, including an issue with control channel input handling and a processing issue with signature records used for DNSSEC validation that may lead to DoS attacks from external sources. A vulnerability in the GNU C Library (glibc) included in Linux distributions that could allow remote code execution was discovered and fixed. This is due to a buffer overflow in a name resolution library function and can be triggered when an attacker sends malicious DNS responses[*17]. Attacks targeting SSL/TLS implementations were also discovered, such as an attack that breaks TLS security through hash collisions (SLOTH), an attack that allows SSLv2 encrypted communications to be decrypted (DROWN), and a timing attack that makes it possible to reconstruct RSA private keys (CacheBleed). These vulnerabilities were fixed in SSL/TLS implementations such as NSS and OpenSSL.

In network devices, vulnerabilities that may allow backdoor access due to fixed passwords being set for administrator accounts were discovered and fixed in both Fortinet and Cisco products. Also in the IKEv1/IKEv2 key exchange protocol, an issue in the

*2 "Microsoft Security Bulletin MS16-003 - Critical: Cumulative Security Update for JScript and VBScript to Address Remote Code Execution (3125540)" (https://technet.microsoft.com/en-us/library/security/MS16-003).
*3 "Microsoft Security Bulletin MS16-005 - Critical: Security Update for Windows Kernel-Mode Drivers to Address Remote Code Execution (3124584)" (https://technet.microsoft.com/en-us/library/security/MS16-005).
*4 "Microsoft Security Bulletin MS16-012 - Critical: Security Update for Microsoft Windows PDF Library to Address Remote Code Execution (3138938)" (https://technet.microsoft.com/en-us/library/security/MS16-012).
*5 "Microsoft Security Bulletin MS16-013 - Critical: Security Update for Windows Journal to Address Remote Code Execution (3134811)" (https://technet.microsoft.com/en-us/library/security/MS16-013).
*6 "Microsoft Security Bulletin MS16-026 - Critical: Security Update for Graphic Fonts to Address Remote Code Execution (3143148)" (https://technet.microsoft.com/en-us/library/security/MS16-026).
*7 "Microsoft Security Bulletin MS16-027 - Critical: Security Update for Windows Media to Address Remote Code Execution (3143146)" (https://technet.microsoft.com/en-us/library/security/MS16-027).
*8 "Microsoft Security Bulletin MS16-028 - Critical: Security Update for Microsoft Windows PDF Library to Address Remote Code Execution (3143081)" (https://technet.microsoft.com/en-us/library/security/MS16-028).
*9 "Microsoft Security Bulletin MS16-001 - Critical: Cumulative Security Update for Internet Explorer (3124903)" (https://technet.microsoft.com/en-us/library/security/MS16-001).
*10 "Microsoft Security Bulletin MS16-009 - Critical: Cumulative Security Update for Internet Explorer (3134220)" (https://technet.microsoft.com/en-us/library/security/MS16-009).
*11 "Microsoft Security Bulletin MS16-023 - Critical: Cumulative Security Update for Internet Explorer (3142015)" (https://technet.microsoft.com/en-us/library/security/MS16-023).
*12 "Microsoft Security Bulletin MS16-004 - Critical: Security Update for Microsoft Office to Address Remote Code Execution (3124585)" (https://technet.microsoft.com/en-us/library/security/MS16-004).
*13 "Microsoft Security Bulletin MS16-015 - Critical: Security Update for Microsoft Office to Address Remote Code Execution (3134226)" (https://technet.microsoft.com/en-us/library/security/MS16-015).
*14 "Microsoft Security Bulletin MS16-002 - Critical: Cumulative Security Update for Microsoft Edge (3124904)" (https://technet.microsoft.com/en-us/library/security/MS16-002).
*15 "Microsoft Security Bulletin MS16-011 - Critical: Cumulative Security Update for Microsoft Edge (3134225)" (https://technet.microsoft.com/en-us/library/security/MS16-011).
*16 "Microsoft Security Bulletin MS16-024 - Critical: Cumulative Security Update for Microsoft Edge (3142019)" (https://technet.microsoft.com/en-us/library/security/MS16-024).
*17 Refer to the following IIJ Security Diary articles for more information. "IIJ Security Diary: CVE-2015-7547 Regarding the getaddrinfo vulnerability in glibc (https://sect.iij.ad.jp/d/2016/02/197129.html) (in Japanese). "IIJ Security Diary: Cache servers that can be trusted for countermeasures to CVE-2015-7547 (https://sect.iij.ad.jp/d/2016/02/225250.html) (in Japanese).

January Incidents

S **6th: DDoS attacks against the website of Donald Trump and on the PlayStation Network, with a group called "New World Hacking" claiming responsibility.**

V **7th: The INRIA Group disclosed an attack method that breaks TLS security using hash collisions, referred to as SLOTH. Fixes that removed RSA-MD5 support were made to multiple implementations.**
"miTLS, Triple Handshake, SMACK, FREAK, Logjam, and SLOTH" (http://www.mitls.org/pages/attacks/SLOTH).

S **12th: The European Police Office (EUROPOL) announced that key members of DD4BC had been arrested through a joint effort involving investigative organizations in multiple European countries.**
"International action against DD4BC cybercriminal group | Europol"
(https://www.europol.europa.eu/content/international-action-against-dd4bc-cybercriminal-group).

V **12th: Multiple vulnerabilities in Adobe Acrobat and Reader that could allow unauthorized termination and arbitrary code execution were discovered and fixed.**
"APSB16-02: Security Updates Available for Adobe Acrobat and Reader" (https://helpx.adobe.com/security/products/acrobat/apsb16-02.html).

O **12th: The JPCERT Coordination Center published an alert regarding the risk of information leaks due to misconfigured DNS zone transfer after they received word that zone information could be obtained from multiple authoritative DNS servers in Japan.**
"Alert regarding possible information leakage due to improper DNS zone transfer settings" (http://www.jpcert.or.jp/english/at/2016/at160002.html).

V **13th: Microsoft published their Security Bulletin Summary for January 2016, and released a total of nine updates, including six critical updates such as MS16-001, as well as three important updates.**
"Microsoft Security Bulletin Summary for January 2016" (https://technet.microsoft.com/library/security/ms16-jan).

S **13th: An extortion attempt with financial demands took place, against a Japanese company after its Web server was accessed without authorization and a list of customer information stolen.**

S **13th: Websites of the Nissan Motor Group were targeted in DDoS attacks by Anonymous, causing them to be temporarily inaccessible (OpKillingBay).**

S **13th: The hacker group that hijacked the email account of CIA Director John Brennan in 2015 also hijacked the email accounts of Director of National Intelligence James Clapper and others.**

O **15th: Microsoft announced that support for Windows 7 / 8.1 will end on July 17, 2017 for PCs and tablets equipped with Intel's latest 6th generation Core (development codename Skylake) CPUs.**
"Windows 10 Embracing Silicon Innovation | Windows Experience Blog"
(https://blogs.windows.com/windowsexperience/2016/01/15/windows-10-embracing-silicon-innovation/).

V **19th: Apple released iOS 9.2.1, OS X El Capitan 10.11.3, and Security Update 2016-001, fixing multiple vulnerabilities, including one that could allow a local user to gain elevated privileges and execute arbitrary code.**
"About the security content of iOS 9.2.1 - Apple Support" (https://support.apple.com/en-us/HT205732) "About the security content of OS X El Capitan 10.11.3 and Security Update 2016-001 - Apple Support" (https://support.apple.com/en-us/HT205731).

V **20th: Oracle released their quarterly scheduled update for multiple products including Java SE and Oracle Database Server, fixing a total of 248 vulnerabilities.**
"Oracle Critical Patch Update Advisory - January 2016" (http://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html).

S **23rd: The personal website of Prime Minister Shinzo Abe was targeted in DDoS attacks by Anonymous, causing it to be temporarily inaccessible (OpKillingBay).**

O **26th: The 6th assembly of the Cyber Security Strategic Headquarters was held, and policies regarding further functional enhancements for promoting cyber security were determined.**
National center of Incident readiness and Strategy for Cybersecurity, "Policies regarding further functional enhancements for promoting cyber security in Japan" (http://www.nisc.go.jp/active/kihon/pdf/cs_kyoka_hoshin.pdf) (in Japanese).

S **31st: The websites of the Financial Services Agency, the Ministry of Finance, and the House of Representatives were targeted in DDoS attacks by Anonymous, causing them to be temporarily inaccessible (OpKillingBay).**

*Dates are in Japan Standard Time

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

protocol specification was discovered. This issue may lead to a device becoming a source for DoS attacks by amplifying the amount of data transferred. Vendors with affected devices have provided firmware updates and workarounds for this issue*18.

■ Escalating Damages Due to Ransomware

Since the second half of last year, damages caused by ransomware infections have been escalating in Japan and overseas, and this trend continued over the current survey period. Ransomware is a type of malware also referred to as a "virus that demands a ransom." When an infection occurs, certain types of files on the computer are encrypted and held hostage. The user is then demanded to make a payment in the form of Bitcoin or other currency in exchange for the key to decrypt these files. Various ransomware such as TeslaCrypt, Locky, Samas, and Petya have become extremely prevalent, and infections have spread within corporate organizations and to individual users. Of particular note during the current survey period was a large number of reports of infections at hospitals overseas. In February, a number of computers at a hospital in Los Angeles in the United States were infected with ransomware, interfering with medical activities. It has been reported that to prioritize restoring operations at the hospital, a total ransom of 40 BTC (approximately US$17,000) was paid. Losses due to ransomware infections have also been confirmed at hospitals in Germany and New Zealand. In light of these developments, US-CERT issued an alert regarding ransomware in March, urging for measures such as the backup of data to be taken. On the other hand, due to this market suddenly appearing, in many cases the ransomware is of poor quality and uses flawed encryption mechanisms, so for some variants files can be restored without paying the ransom. See "1.4.1 Various Ransomware and Their Countermeasures" for more information about ransomware.

■ Government Agency Initiatives

Following on from last year, the government designated the period between February 1 and March 18 as "Cyber Security Month," and focused on promoting public awareness activities regarding cyber security through the cooperation of government agencies and a wide range of other related institutions and organizations*19.

The Ministry of Internal Affairs and Communications announced the February launch of an initiative for preventing damages caused by those infected with malware through their "public-private collaboration project to support malware countermeasures in Japan (Advanced Cyber Threats response InitiatiVE (abbreviated as 'ACTIVE'))." Information regarding C&C servers obtained through ACTIVE is provided to Internet Service Providers (ISPs) in Japan in coordination with the Telecom Information Sharing and Analysis Center Japan. Each ISP uses this information to block communications between malware and C&C servers, and also issues alerts to users of malware-infected PCs to reduce the damage caused. This initiative is based on the content of the "Second Report of the Workshop on the Appropriate Way for Telecommunications Organizations to Handle Cyber Attacks"*20 published by the Ministry of Internal Affairs and Communications last year.

Also in February, a cabinet decision was made on the "Bill for Partial Revisions to the Basic Act on Cyber Security and the Act on Facilitation of Information Processing." This was submitted to the 190th Regular Diet Session, and following deliberation by both houses the bill was passed on April 14. Through these revisions the scope of information system monitoring at administrative bodies by the National center of Incident readiness and Strategy for Cybersecurity (NISC) will expand beyond central government ministries to include independent administrative institutions and designated corporations, increasing oversight in stages. A new "Information Processing Security Supporter" national qualification will also be established for those providing cyber security advice.

*18 Akamai's Security Intelligence Research Team, "White Paper_IKE_IKEv2 - ripe for DDoS abuse" (https://community.akamai.com/docs/DOC-5289).
*19 National center of Incident reading and Strategy for Cybersecurity (NISC), "Regarding Cyber Security Month 2016" (http://www.nisc.go.jp/press/pdf/csm2016_press1.pdf) (in Japanese).
*20 Ministry of Internal Affairs and Communications, "'Second Report of the Workshop on the Appropriate Way for Telecommunications Organizations to Handle Cyber Attacks' and Results of Request for Public Comment Published" (http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000100.html) (in Japanese).

February Incidents

S **1st: The police report on a second year high school student suspected of storage of electromagnetic records of a computer virus, for storing Zeus malware on their home computer, was forwarded to a prosecutor.**

V **2nd: A vulnerability that allows authentication functions to be circumvented was discovered and fixed in toys produced by Fisher-Price. Affected are an educational toy for infants called Smart Toy and a GPS watch for kids called hereO.**
"Vulnerability Note VU#719736: Fisher-Price Smart Toy platform allows some unauthenticated web API commands" (http://www.kb.cert.org/vuls/id/719736).

S **2nd: A former employee of a financial service provider in Japan took more than 18 sets of customer data as well as trade secrets off company premises without permission and stored them on the Internet. This information was publicly viewable by third parties.**

O **2nd: The Japanese government made a cabinet decision regarding the "Bill for Partial Revisions to the Basic Act on Cyber Security and the Act on Facilitation of Information Processing," and submitted it to the Diet.**
Cabinet Secretariat, "Bill for Partial Revisions to the Basic Act on Cyber Security and the Act on Facilitation of Information Processing" submitted to the 190th ordinary session of the National Diet (http://www.cas.go.jp/jp/houan/190.html) (in Japanese).

O **3rd: The European Commission and the United States reached an agreement regarding the introduction of a new "EU-US Privacy Shield" framework for data transfer to replace the Safe Harbor Framework.**
European Commission, "EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield" (http://europa.eu/rapid/press-release_IP-16-216_en.htm).

O **6th: Twitter announced they had frozen 125,000 accounts related to terrorist activities since mid-2015.**
"Combating Violent Extremism | Twitter Blogs" (https://blog.twitter.com/2016/combating-violent-extremism).

V **9th: Multiple vulnerabilities in Adobe Flash Player that could allow unauthorized termination or arbitrary code execution were discovered and fixed.**
"APSB16-04: Security updates available for Adobe Flash Player" (https://helpx.adobe.com/security/products/flash-player/apsb16-04.html).

S **9th: The hacker group that hijacked the account of the U.S. CIA Director and the Director of National Intelligence compromised a computer at the U.S. Department of Justice and obtained and published information on tens of thousands of federal employees without authorization. Members of this hacker group were subsequently arrested in rapid succession in the United Kingdom and other countries.**

V **10th: Microsoft published their Security Bulletin Summary for February 2016, and released a total of thirteen updates, including six critical updates such as MS16-009, as well as seven important updates.**
"Microsoft Security Bulletin Summary for February 2016" (https://technet.microsoft.com/library/security/ms16-feb).

S **10th: The websites of Japan Securities Finance Co.,Ltd., the National Tax Administration Agency, and the Japan External Trade Organization were targeted in DDoS attacks by Anonymous, causing them to be temporarily inaccessible (OpKillingBay).**

V **17th: A vulnerability in the glibc library that could allow remote code execution through a buffer overflow was discovered and fixed.**
"Google Online Security Blog: CVE-2015-7547: glibc getaddrinfo stack-based buffer overflow" (https://security.googleblog.com/2016/02/cve-2015-7547-glibc-getaddrinfo-stack.html).

O **17th: A federal court ordered Apple to provide technical support to enable the FBI to unlock an iPhone belonging to a perpetrator of the San Bernardino shooting, but Apple refused to comply with the order.**
"Apple Litigation | USAO-CDCA | Department of Justice" (https://www.justice.gov/usao-cdca/apple-litigation).

S **18th: Multiple computers at a hospital in Los Angeles, United States, were infected with ransomware, greatly impacting medical activities. Swift restoration of their system was prioritized and they paid a total ransom of 40 BTC (approximately US$17,000).**
Hollywood Presbyterian Medical Center
(http://hollywoodpresbyterian.com/default/assets/File/20160217%20Memo%20from%20the%20CEO%20v2.pdf)

S **19th: A crackdown on copyright infringement through the use of file sharing software was implemented by police in 29 prefectures. 93 locations were searched, resulting in the arrest of 44 individuals nationwide.**
National Police Agency, "Regarding the crackdown on copyright infringement through the use of file sharing software" (http://www.npa.go.jp/cyber/warning/h28/H280219.pdf) (in Japanese).

S **22nd: A server for the Linux Mint distribution of Linux was compromised by an external party, and an ISO image file containing malware was temporarily made available to the public. The database for the user forum was also compromised, leading to the leak of account information such as email addresses and encrypted passwords.**
The Linux Mint Blog, "Beware of hacked ISOs if you downloaded Linux Mint on February 20th!" (http://blog.linuxmint.com/?p=2994). The Linux Mint Blog, "All forums users should change their passwords." (http://blog.linuxmint.com/?p=3001).

O **26th: The Ministry of Internal Affairs and Communications announced they had launched an initiative for preventing damages caused by those infected with malware through a "public-private project to support malware countermeasures in Japan (Advanced Cyber Threats response InitiatiVE (abbreviated as 'ACTIVE'))."**
Ministry of Internal Affairs and Communications, "Preventing malware damage before it occurs" (http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000106.html) (in Japanese).

*Dates are in Japan Standard Time

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

Other

In February, interest was generated when a federal court ordered Apple to provide technical support to enable the FBI to unlock an iPhone that was in possession of one of the perpetrators of the shooting that took place in San Bernardino in the United States in December 2015. The latest version of iOS is designed to prevent even the manufacturer, Apple, from unlocking or extracting data from an iPhone. So the FBI, in an attempt to brute force the passcode to unlock the device, requested Apple to create special software to disable the protection against such brute force attempts. Apple responded by rejecting the court order and indicating they would take the dispute to court. However, in March the FBI was able to unlock the phone using a different method. As a result the lawsuit was withdrawn, bringing the matter to a close. But the method that the FBI used to successfully unlock the phone does not work against the latest iPhone models, and similar requests have already been made to Apple in relation to other investigations. Furthermore, there has been movement in U.S. Congress to introduce legislation that will require technology companies to decrypt data, so future trends surrounding cryptographic regulations will be watched with considerable interest.

During the current survey period there were ongoing unauthorized login attempts thought to have used lists of IDs and passwords obtained from other sites. Targets included loyalty program and game sites. These incidents resulted in financial losses such as the unauthorized exchange of loyalty points through the website.

Phishing incidents reported to the Council of Anti-Phishing Japan have risen sharply since last December. In particular, phishing attempts fraudulently using the names of multiple financial institutions occurred in February, resulting in the number of incidents reported in February rising to 2,935*21. It was discovered that incidents at some financial institutions involved redirection to phishing sites via SMS rather than phishing emails, so ongoing caution is required.

In February, illegal money transfers totaling in excess of 100 million dollars took place at the Bangladesh Bank, resulting in the largest ever financial loss suffered by a single bank. The perpetrators accessed the bank's internal system without authorization, and issued instructions to transfer money to bank accounts in the Philippines and Sri Lanka from a foreign exchange account of the Bangladesh Bank managed by the Federal Reserve Bank of New York. The illegal transactions were discovered due to a spelling mistake in the remittee account name, but over 100 million dollars had already been transferred by that point, the majority of which has yet to be recovered.

In October 2015, there were incidents where a hacker group hijacked accounts belonging to a number of U.S. government officials, including the AOL email account of CIA Director John Brennan. This group hijacked an account belonging to U.S. Director of National Intelligence James Clapper in January. In February, they compromised the computer of a U.S. Department of Justice staff member and then published the illegally obtained information on tens of thousands of federal employees on an Internet website. A number of members of this group were subsequently arrested in quick succession in the United Kingdom and other countries, but all were teenagers. They used social engineering techniques skillfully to compromise the systems. For example, they posed as an engineer from the telecommunications company Verizon, which the CIA Director uses, and phoned Verizon to elicit his personal account details, which were used to reset the password for his email account. They also phoned a help desk posing as a Department of Justice employee, and obtained a token necessary to compromise a computer. It is difficult to prevent attack techniques such as these through technical measures alone, so there is a need for multi-layered countermeasures, such as the preparation and application of information disclosure rules, as well as education that also take into account human shortcomings.

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 do not utilize advanced knowledge such as vulnerabilities, but aim to hinder or delay services by causing large volumes of unnecessary traffic to overwhelm network bandwidth or server processes.

*21 Council of Anti-Phishing Japan, "2016/02 Phishing Report Status" (https://www.antiphishing.jp/report/monthly/201602.html) (in Japanese).

March Incidents

S **1st: It was confirmed that user email addresses and plain text passwords for approximately 27 million individuals had leaked from the online dating site Mate1.com, and were being offered for sale on a Dark Web message board.**

V **1st: Researchers disclosed an attack against SSLv2 where encrypted communications can be decrypted, referred to as the DROWN attack method, and an attack where RSA keys can be recovered through timing attacks, referred to as the CacheBleed attack method. These vulnerabilities were fixed in OpenSSL versions 1.0.2g and 1.0.1s.**
"DROWN Attack" (https://drownattack.com/). "CacheBleed: A Timing Attack on OpenSSL Constant Time RSA" (https://ssrg.nicta.com.au/projects/TS/cachebleed/). "OpenSSL Security Advisory [1st March 2016]" (https://www.openssl.org/news/secadv/20160301.txt).

S **3rd: Incidents of unauthorized logins through identity fraud took place at an Internet shopping site in Japan, resulting in the unauthorized use of loyalty points.**

O **3rd: The U.S. Department of Defense announced the "Hack the Pentagon" bug bounty program (a system offering monetary rewards for the discovery of vulnerabilities). This was the first time a federal government institution proposed such a program.**
U.S. Department of Defense, "Statement by Pentagon Press Secretary Peter Cook on DoD's "Hack the Pentagon" Cybersecurity Initiative" (http://www.defense.gov/News/News-Releases/News-Release-View/Article/684106/statementby-pentagon-press-secretary-peter-cook-on-dods-hack-the-pentagon-cybe).

V **8th: Multiple vulnerabilities in Adobe Acrobat and Reader that could allow unauthorized termination and arbitrary code execution were discovered and fixed.**
"APSB16-09: Security Updates Available for Adobe Acrobat and Reader" (https://helpx.adobe.com/security/products/acrobat/apsb16-09.html).

V **9th: Microsoft published their Security Bulletin Summary for March 2016, and released a total of fourteen updates, including six critical updates such as MS16-023, as well as eight important updates.**
"Microsoft Security Bulletin Summary for March 2016" (https://technet.microsoft.com/library/security/ms16-mar).

V **10th: Multiple vulnerabilities in Adobe Flash Player that could allow unauthorized termination or arbitrary code execution were discovered and fixed.**
"APSB16-08: Security updates available for Adobe Flash Player" (https://helpx.adobe.com/security/products/flash-player/apsb16-08.html).

O **17th: The National Police Agency released a report on the state of cyberspace threats for 2015. The Agency states that the number of reported targeted email attacks increased dramatically, reaching a record high, and the total amount of financial losses due to illegal Internet banking transactions was also the highest ever.**
National Police Agency, "Report on Cyberspace Threats for 2015" (http://www.npa.go.jp/kanbou/cybersecurity/H27_jousei.pdf) (in Japanese).

V **21th: Apple released iOS 9.3, OS X El Capitan 10.11.4, and Security Update 2016-002, fixing multiple vulnerabilities, including those that could allow a remote attacker to execute arbitrary code.**
"About the security content of iOS 9.3 - Apple Support" (https://support.apple.com/en-us/HT206166) "About the security content of OS X El Capitan 10.11.4 and Security Update 2016-002 - Apple Support" (https://support.apple.com/en-us/HT206167).

V **24th: A vulnerability (CVE-2016-0636) in Oracle Java SE that could allow remote execution of arbitrary code was discovered and fixed.**
"Oracle Security Alert for CVE-2016-0636" (http://www.oracle.com/technetwork/topics/security/alert-cve-2016-0636-2949497.html).

S **25th: The U.S. Department of Justice announced that it had prosecuted seven Iranians for carrying out cyber attacks on the control system of a dam in New York state as well as major financial institutions.**
Department of Justice, "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector" (https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged).

O **31st: The JPCERT Coordination Center published a guide to be used by companies and organizations for preparing against advanced persistent threats (APT).**
"A guide for preparing against advanced persistent threats (APT) - a series of process recommendations for companies and organizations" (https://www.jpcert.or.jp/research/apt-guide.html) (in Japanese).

O **31st: The IPA published their "10 Major Security Threats for 2016," which summarizes threats of note as chosen by experts in the field of information security.**
"10 Major Security Threats for 2016" (https://www.ipa.go.jp/security/vuln/10threats2016.html) (in Japanese).

O **31st: US-CERT issued an alert due to the worldwide spread of ransomware infections at hospitals and other organizations.**
"Ransomware and Recent Variants" (https://www.us-cert.gov/ncas/alerts/TA16-091A).

*Dates are in Japan Standard Time

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

Direct Observations

Figure 2 shows the state of DDoS attacks handled by the IIJ DDoS Protection Service between January 1 and March 31, 2016.

This shows the number of traffic anomalies judged to be attacks based on IIJ DDoS Protection Service criteria. IIJ also responds to other DDoS attacks, but these incidents have been excluded here due to the difficulty in accurately understanding and grasping the facts behind such attacks.

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 splits DDoS attacks into three categories: attacks against bandwidth capacity*22, attacks against servers*23, and compound attacks (several types of attacks against a single target conducted at the same time).

During these three months, IIJ dealt with 293 DDoS attacks. This averages out to 3.22 attacks per day, which is a significant decrease in comparison to our prior report. Server attacks accounted for 59.04% of DDoS attacks, while compound attacks accounted for 38.91%, and bandwidth capacity attacks 2.05%.

The largest scale attack observed during this period was classified as a compound attack, and resulted in 2.86 Gbps of bandwidth using up to 1,066,000 pps packets.

Of all attacks, 85.67% ended within 30 minutes of the start of the attack, 13.99% lasted between 30 minutes and 24 hours, and 0.34% lasted over 24 hours. The longest sustained attack for this period was a compound attack that lasted for one day, 12 hours, and 26 minutes (36 hours and 26 minutes).

We observed an extremely large number of IP addresses as the attack sources, whether domestic or foreign. We believe this is due to the use of IP spoofing*24 and botnets*25 to conduct the DDoS attacks.

Backscatter Observations

Next we present DDoS attack backscatter observations*26 through the honeypots*27 of the IIJ malware activity observation project, MITF. Through backscatter observations, portions of DDoS attacks against external networks may be detectable as a third-party without intervening.

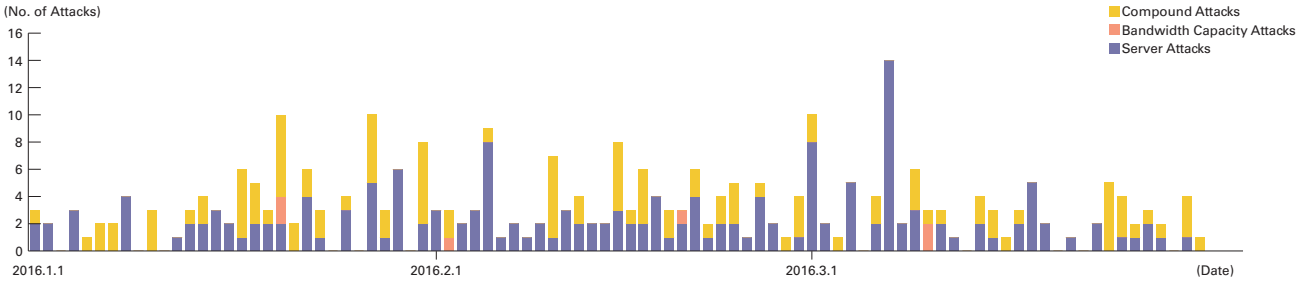


Figure 2: Trends in DDoS Attacks

*22 Attack that overwhelms the network bandwidth capacity of a target by sending massive volumes of larger-than-necessary IP packets and fragments. When UDP packets are used, it is referred to as a UDP flood, while ICMP flood is used to refer to the use of ICMP packets.

*23 TCP SYN flood, TCP connection flood, and HTTP GET flood attacks. In a TCP SYN flood attack, a large number of SYN packets that signal the start of TCP connections are sent, forcing the target to prepare for a large number of incoming connections, resulting in the waste of processing capacity and memory. TCP connection flood attacks establish a large number of actual TCP connections. In a HTTP GET flood a TCP connection with a Web server is established, and then a large number of GET requests in the HTTP protocol are sent, also resulting in a waste of processing capacity and memory.

*24 Impersonation of a source IP address. Creates and sends an attack packet that has been given an IP address other than the actual IP address used by the attacker to make it appear as if the attack is coming from a different person, or from a large number of individuals.

*25 A "bot" is a type of malware that after infection, conducts an attack upon receiving a command from an external C&C server. A network made up from a large number of bots is called a botnet.

*26 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 (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol08_EN.pdf) under "1.4.2 Observations on Backscatter Caused by DDoS Attacks."

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

For the backscatter observed between January 1 and March 31, 2016, Figure 3 shows the source IP addresses classified by country, and Figure 4 shows trends in the number of packets by port.

The port most commonly targeted by DDoS attacks observed was port 53/UDP used for DNS, and accounted for 49.5% of the total. This was followed by 80/TCP used for Web services at 18.6%, so the top two ports alone accounted for 68.1% of the total. Attacks were also observed on 53/TCP used for DNS, 2401/TCP used by servers running the CVS version control system, 443/TCP used for HTTPS, and both 27015/UDP and 25565/TCP that are sometimes used for gaming communications, as well as typically unused ports such as 83/TCP, 43783/TCP, and 7829/TCP.

Communications at 53/UDP, which have been observed often since February 2014, remained high, and the average daily number of packets observed was around 5,300.

Looking at the source of backscatter packets by country thought to indicate IP addresses targeted by DDoS attacks in Figure 3, the United States accounted for the largest percentage at 20.5%, while China and France followed at 20.1% and 9.0%, respectively.

Now we will take a look at ports targeted in attacks where a large number of backscatter packets were observed. For attacks against Web servers (80/TCP and 443/TCP), there were intermittent attacks starting from November 27, 2015 from the last survey period through February 25 targeting a data center provider in the Netherlands. We also observed attacks against a non-profit organization in France during two periods, January 14 through January 20, and February 2 through February 13. There were also attacks observed against the servers of a hosting provider in China from January 28 through March 10, and against the Arizona state court from March 26 through March 31. Attacks against other ports included those targeting 53/TCP again, as observed during the last survey period against multiple DNS servers of a U.S. CDN provider on January 2 and from January 19 through February 1. There were also attacks against 2401/TCP targeting a specific IP address allocated to a communications provider in Croatia from February 6 through March 16, as well as those against 83/TCP targeting a corporate website in Poland from February 27 through March 4, and March 28 through March 29. We also observed attacks against 7829/TCP targeting a specific IP address allocated to an ISP in Bangladesh between March 11 and March 24.

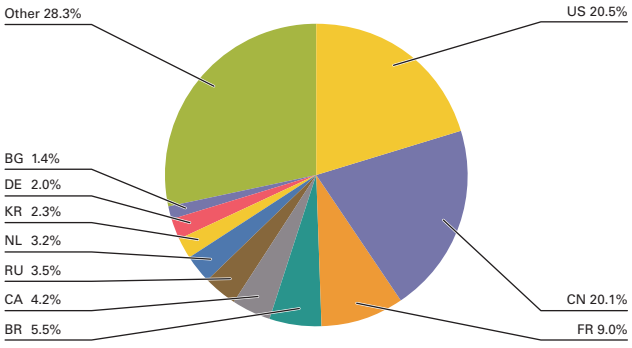


Figure 3: DDoS Attack Targets by Country According to Backscatter Observations

Notable DDoS attacks during the current survey period that were detected by IIJ's backscatter observations included intermittent attacks against the websites of a candidate in the U.S. presidential primary elections, and attacks against the Saudi Arabian Ministry of Defense from January 3 through January 5. There were also attacks against the Irish government from January 22 through January 24, and attacks targeting the website of a Japanese airport company on January 22 and January 25. Attacks were also detected against the website of the Salt Lake City Police Department in the United States on March 13.

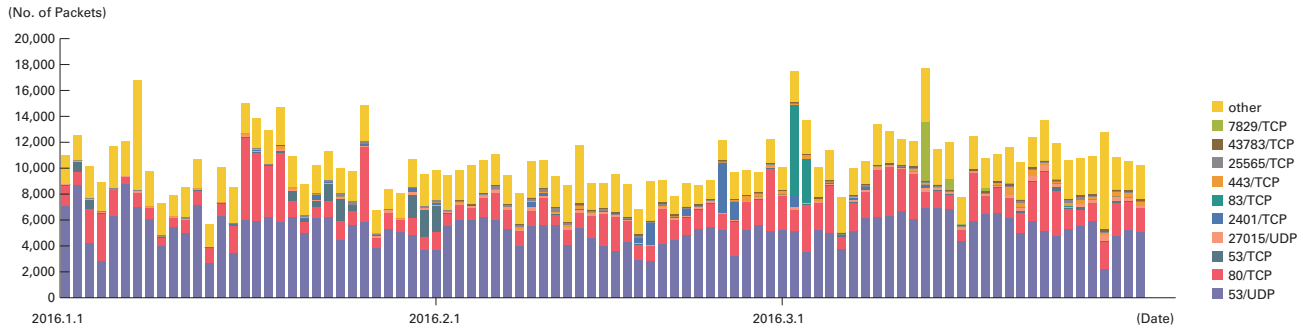


Figure 4: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the MITF*28, the malware activity observation project operated by IIJ. The MITF uses honeypots*29 connected to the Internet in a manner similar to general users in order to observe communications that arrive over the Internet. Most appear to be communications by malware selecting a target at random, or scans attempting to search for a target to attack.

Status of Random Communications

Figure 5 shows the distribution of source IP addresses by country for incoming communications to the honeypots from January 1 through March 31, 2016. Regarding the total volume (incoming packets), because communications to 53/UDP were significantly higher than other ports during the survey period for this report, we have plotted trends for 53/UDP on Figure 6, while other ports are shown on Figure 7. The MITF has set up numerous honeypots for its observations. Here, we have taken the average number per honeypot, and shown the trends by country in Figure 6, and trends for incoming packet types (top ten) in Figure 7. Additionally, in these observations we made an adjustment so that multiple TCP connections are counted as one attack, in cases such as attacks against MSRPC in which multiple connections to a specific port are involved.

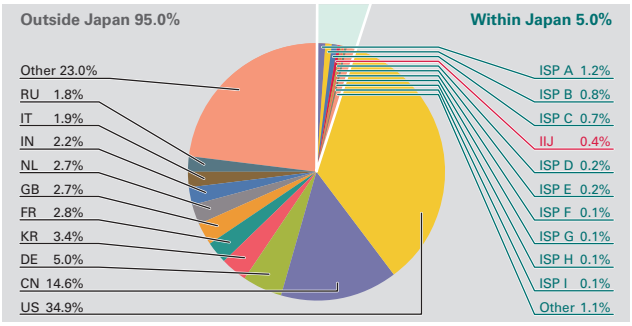


Figure 5: Sender Distribution (by Country, Entire Period under Study)

As with the survey period for the previous report, there was a high number of 53/UDP communications. Upon investigating these communications, DNS name resolution requests from a range of source IP addresses allocated mainly to the United

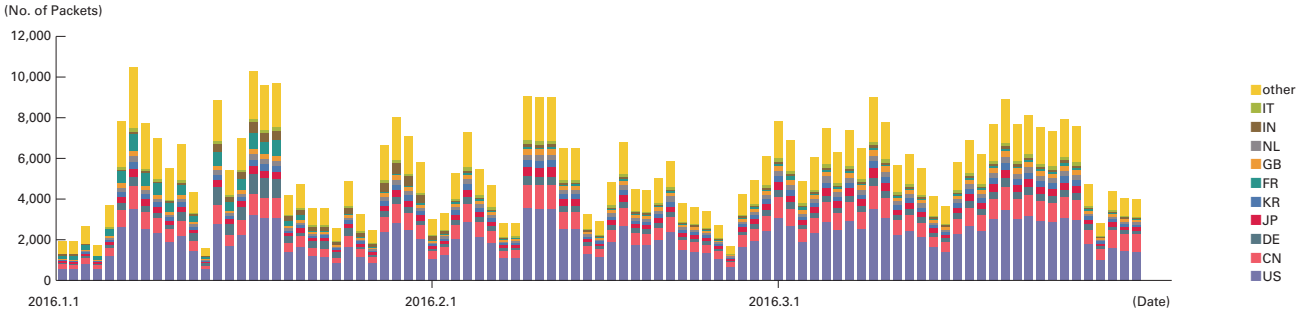


Figure 6: Incoming Communications at Honeypots (by Date, 53/UDP, per Honeypot)

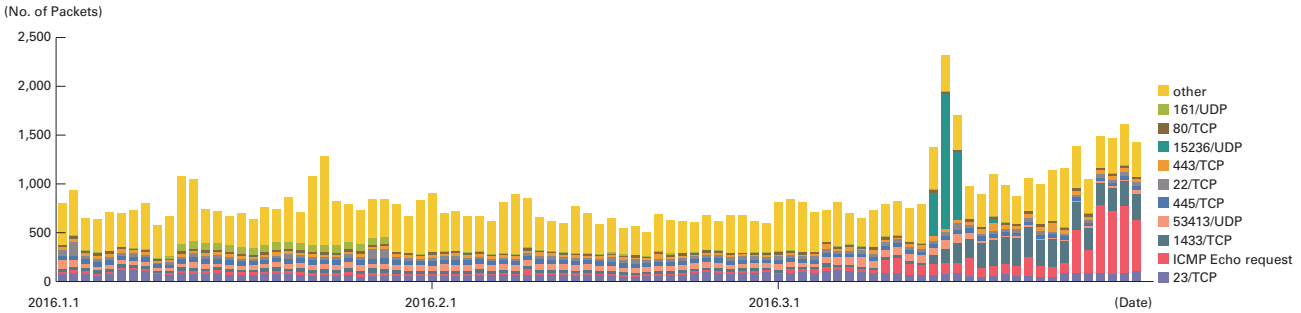


Figure 7: Incoming Communications at Honeypots (by Date, by Target Port, per Honeypot)

*28 An abbreviation of Malware Investigation Task Force. The Malware Investigation Task Force (MITF) began its activities in May 2007, observing malware activity in networks through the use of honeypots in an attempt to understand the state of malware activities, to collect technical information for countermeasures, and to link these findings to actual countermeasures.

*29 A system designed to record attacker and malware activities and their behavior by emulating vulnerabilities and simulating the damages caused by attacks.

States and China were being repeatedly received on the IP address of a certain MITF honeypot. Multiple corresponding domain names were also confirmed, and many were sites related to online shopping, games, and science fiction novels in China. Because the majority of these communications involved repeated name resolution attempts for "(random).(existing domain)," we believe these to be DNS water torture attacks*30.

From March 17, the number of ICMP echo requests and 1433/TCP communications increased. Upon investigation, we determined that a large number of these communications were from IP addresses chiefly allocated to China, as well as many other IP addresses.

During the current survey period, 53413/UDP communications increased. We found that these communications were attacks targeting a vulnerability in Netis and Netcore brand routers. The vulnerability was reported by Trend Micro in August 2014*31, and JPCERT/CC reported there was a spike in attacks between April and June of 2015*32.

Between mid- and late January, there was an increase in SNMP traffic from Japanese IP addresses. Our investigations indicated that these were repeated requests for information from Yamaha brand routers, such as the CPU utilization and uptime, and the number of bytes transferred.

■ Malware Activity in Networks

Figure 8 shows the distribution of the source where malware artifacts were acquired from during the period under study, while Figure 9 shows trends in the total number of malware artifacts acquired. Figure 10 shows trends in the number of unique artifacts. In Figure 9 and Figure 10, the trends in the number of acquired artifacts show the actual number of artifacts acquired per day*33, while the number of unique artifacts is the number of artifact variants categorized in accordance with their hash digests*34. Artifacts are also identified using anti-virus software, and a color-coded breakdown of the top 10 variants is shown along with the malware names. As with our previous report, for Figure 9 and Figure 10 we have detected Conficker using multiple anti-virus software packages, and removed any Conficker results when totaling data.

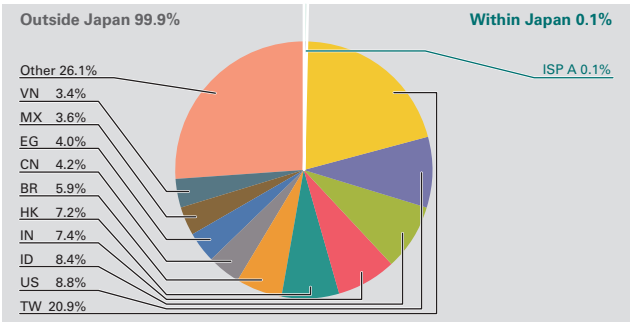


Figure 8: Distribution of Acquired Artifacts by Source (by Country, Entire Period under Study, Excluding Conficker)

*30 Secure64 Software Corporation, "Water Torture: A Slow Drip DNS DDoS Attack" (https://blog.secure64.com/?p=377). For an explanation in Japanese, refer to the following document written by Mr. Yasuhiro Orange Morishita of Japan Registry Services. "DNS Water Torture Attacks" (http://2014.seccon.jp/dns/dns_water_ torture.pdf) (in Japanese). The MITF honeypots do not query authoritative servers or cache servers when they receive DNS query packets, so they do not become a part of attacks.

*31 "Netis Routers Leave Wide Open Backdoor" (http://blog.trendmicro.com/trendlabs-security-intelligence/netis-routers-leave-wide-open-backdoor/)

*32 "JPCERT/CC Internet Threat Monitoring Report [April 1, 2015 - June 30, 2015]" (http://www.jpcert.or.jp/english/doc/TSUBAMEReport2015Q1_en.pdf).

*33 This indicates malware acquired by honeypots.

*34 This value is calculated by utilizing a one-way function (hash function) that outputs a fixed-length value for each input. Hash functions are designed to produce a different output for practically every different input. We cannot guarantee the uniqueness of artifacts through hash values alone, given that obfuscation and padding may result in artifacts of the same malware having different hash values. The MITF understands this fact while using this method as a measurement index.

On average, 91 artifacts were acquired per day during the period under study, while there were 14 unique artifacts per day. After investigating the undetected artifacts more closely, they included worms observed from IP addresses allocated to countries such as Taiwan*35, and Trojans observed from IP addresses allocated to India*36.

About 58% of undetected artifacts were in text format. Many of these text format artifacts were HTML 404 or 403 error responses from Web servers, we believe these were due to infection activities of old malware such as worms continuing despite the closure of download sites that newly-infected PCs access to download malware. A MITF independent analysis revealed that during the current period under observation 89.6% of malware artifacts acquired were worms, 7.8% were bots, and 2.6% were downloaders. In addition, the MITF confirmed the presence of 7 botnet C&C servers*37.

Conficker Activity

Including Conficker, an average of 11,902 artifacts were acquired per day during the period under study for this report, representing 428 unique artifacts. Conficker accounted for 99.5% of the total artifacts acquired, and 96.8% of the unique artifacts. Since Conficker remains the most prevalent malware by far, we have omitted it from the figures in this report. Compared to the previous survey period, the total number of artifacts acquired in this survey period decreased by approximately 33% and the number of unique artifacts decreased by about 11%. There was a gradual overall decrease during the period covered by this report. According to the observations by the Conficker Working Group*38, as of April, 2016, a total of just over 600,000 unique IP addresses are infected. This indicates a drop to about 19% of the 3.2 million PCs observed in November 2011, but it still shows that infections are widespread.

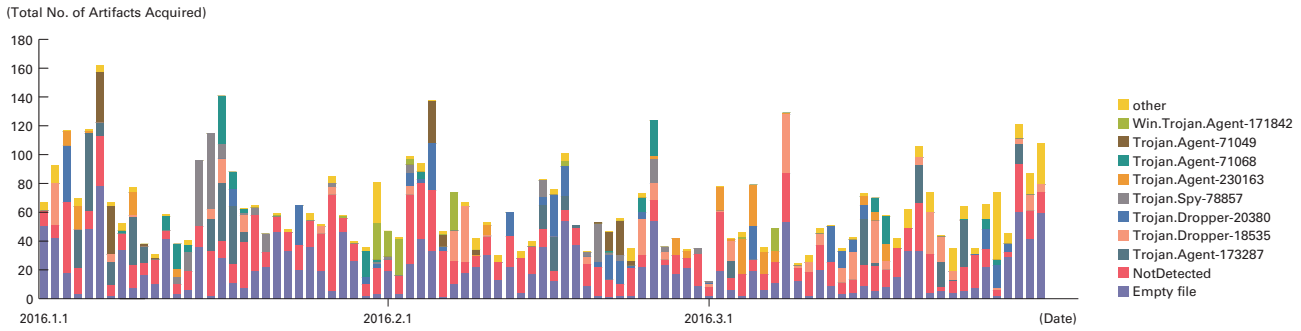


Figure 9: Trends in the Total Number of Malware Artifacts Acquired (Excluding Conficker)

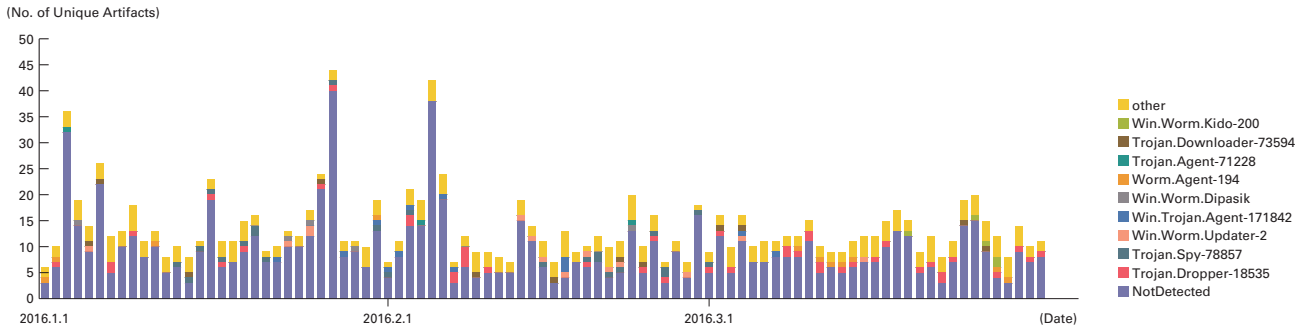


Figure 10: Trends in the Number of Unique Artifacts (Excluding Conficker)

*35 Worm: Win32/Dipasik.A (https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Worm:Win32/Dipasik.A).
*36 Virus: Win32/Ceg.A (https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Virus:Win32/Ceg.A).
*37 An abbreviation of Command & Control Server. A server that provides commands to a botnet consisting of a large number of bots.
*38 Conficker Working Group Observations (http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking). Because no numerical data beyond January 7 is available within the current survey period, we have visually observed the highest value in the graph from early April, and used it.

1.3.3 SQL Injection Attacks

Of the different types of Web server attacks, IIJ is conducting ongoing investigations on to SQL injection attacks*39. SQL injection attacks have been noted a number of times in the past, and continue to remain a major topic in Internet security. SQL injection attacks are known to attempt one of three things: the theft of data, the overloading of database servers, or the rewriting of Web content.

Figure 11 shows the source distribution of SQL injection attacks against Web servers detected between January 1 and March 31, 2016. Figure 12 shows the trend in the number of attacks. These are a summary of attacks detected through signatures in the IIJ Managed IPS Service. Japan was the source for 38.0% of attacks observed, while the United States and China accounted for 27.2% and 24.5%, respectively, with other countries following. Although the number of SQL injection attacks against Web servers from countries other than Japan is in a downward trend since the last report, the number of attacks originating from Japan rose to almost three times the previous figure, so there were more incidents overall.

During this period, attacks from a specific source in the United States directed at specific targets took place on January 25. On March 7, there were attacks from a specific source in China directed at specific targets. Between March 27 and March 29, attacks from a specific source in Japan were detected at specific targets. These attacks are thought to have been attempts to find Web server vulnerabilities.

As previously shown, attacks of various types were properly detected and handled in the scope of the service. However, attack attempts continue, requiring ongoing caution.

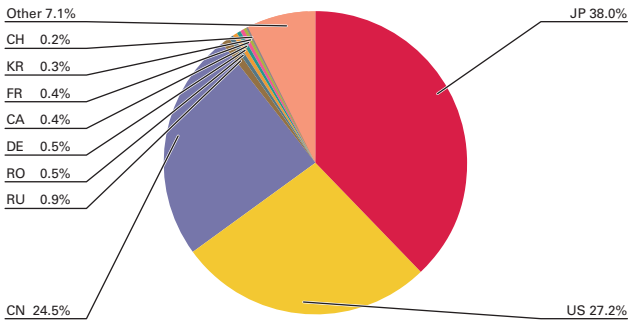


Figure 11: Distribution of SQL Injection Attacks by Source

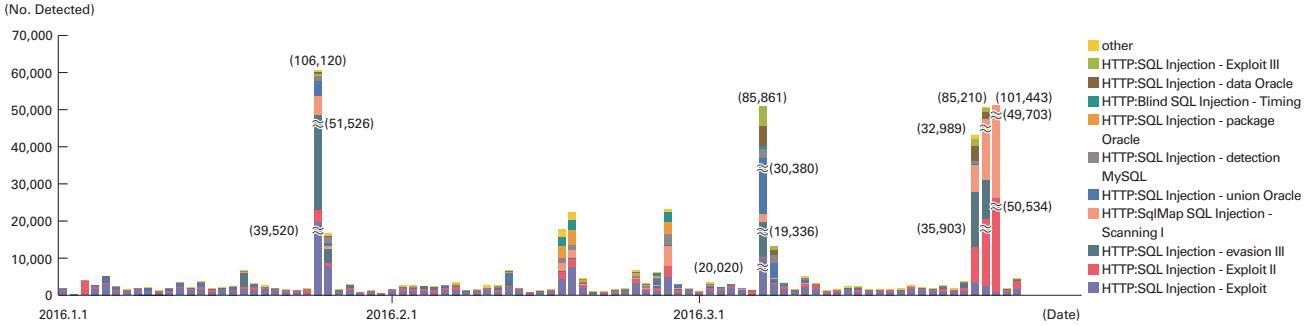


Figure 12: Trends in SQL Injection Attacks (by Day, by Attack Type)

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

1.3.4 Website Alterations

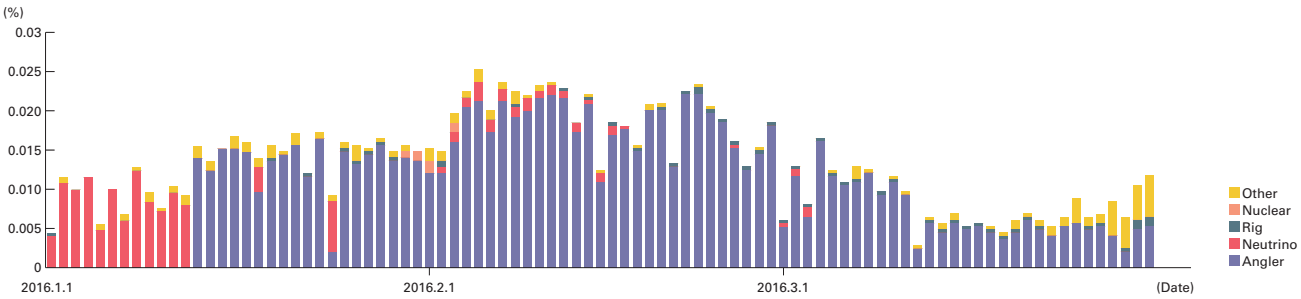
Here we indicate the status of website alterations investigated through the MITF Web crawler (client honeypot)*40.

This Web crawler accesses hundreds of thousands of websites on a daily basis, focusing on well-known and popular sites in Japan. The number of sites that it accesses are added accordingly. In addition to this, we temporarily monitor websites that have seen short- term increases in access numbers. By surveying websites thought to be viewed frequently by typical users in Japan, it becomes easier to speculate on trends for fluctuations in the number of altered sites, as well as the vulnerabilities exploited and malware distributed.

For the period between January 1 and March 31, 2016, Angler accounted for the majority of drive-by download attacks detected (Figure 13). This trend has continued since July 2015*41. However, for 12 days from New Year's Day no Angler-based attacks were detected at all, while Neutrino was detected instead. We have observed Angler and Neutrino trends switching temporarily several times since July 2015, but there had never been such a long period like this where Angler was not detected at all. Angler-based attacks have accounted for the majority throughout most of the entire period since mid-January. Nuclear and Rig attacks have also been observed. Nuclear was small-scale and temporary, while Rig was small-scale, but observed throughout this period. In addition to these exploit kits, we observed incidents in which users were directed to fraudulent sites that prompted them to install scamware or adware or call fake support centers by displaying fake dialog boxes that suggested there was a fault with their PC. These trends have been ongoing for quite some time.

CryptoWall 4.0 initially accounted for the majority of the downloaded malware, but since mid-February TeslaCrypt 3.0 took its place. Malware such as Necurs, Bedep, Locky, and Andromeda were also detected, but only in small numbers. Locky was also ransomware that spread infections through email during the same period*42*43, but it was only detected as the payload of a drive-by download in a few cases, and for a short period of time.

The number of drive-by download attacks is continuing to rise. Website operators must take measures to prevent the alteration of Web content, and properly manage the mashup content provided by external third parties, such as advertisements and Web analytic services. We recommend that they stay aware of the security policies and reputations of content providers. It is also important for browser users and administrators to check for vulnerabilities in OSes and browser-related plug-ins, apply updates, and enable EMET, so that countermeasures are thoroughly applied*44.



*Covers several hundreds of thousands of sites in Japan. In recent years, drive-by downloads have been configured to change attack details and even whether or not to attack based on the client system environment or session information, source address attributes, and an attack quota such as the number of attacks. This means that results can vary wildly depending on the test environment and other circumstances.

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

*40 Refer to "1.4.3 Website Defacement Surveys Using Web Crawlers" in Vol.22 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol22_EN.pdf) for a description of Web crawler observation methods.

*41 Refer to "1.4.2 Angler Exploit Kit on the Rampage" in Vol.28 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol28_EN.pdf) for more information about our observations of the status and functions of Angler in July 2015.

*42 The threat that Locky poses via email was reported in the Symantec blog post "Locky ransomware on aggressive hunt for victims" (http://www.symantec.com/connect/blogs/locky-ransomware-aggressive-hunt-victims).

*43 Ransomware that spreads primarily through drive-by downloads is discussed under "1.4.1 Various Ransomware and Their Countermeasures" in this report.

*44 Refer to "1.4.2 Hardening Windows Clients Against Malware Infections (Part 1)" in this report for more information on countermeasures for malware infections in browser environments.

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 conduct independent surveys and analyses of prevalent incidents. Here, we present information from the surveys we have conducted during this period, covering various ransomware and their countermeasures, hardening Windows clients against malware infections (part 1), and trends in post-quantum cryptography.

1.4.1 Various Ransomware and Their Countermeasures

Ransomware is a generic term for malware that causes files on a computer to become unusable, by encrypting files on the computer where it has been executed. It then displays a threat message demanding some form of a payment, such as money, Bitcoin, or an Amazon or iTunes Store gift card in exchange for restoring (decrypting) the files. Sometimes, the threat messages displayed match the language corresponding to the user's environment. For example, Locky displays messages in Japanese as shown in Figure 14. This type of malware has been known since around 1989*45, and starting with PGPCoder*46 that made headlines in 2005, it has become a recurring topic of interest. In this report we will provide an overview of ransomware collected by the MITF's Web crawler system between October 2015 and March 2016, introduce the functions of the ransomware, and then discuss how to handle and take countermeasures.

■ Ransomware Trends

Figure 15 shows the types and number of ransomware detected by IIJ's Web crawler system between October 2015 and March 2016, and a list of ransomware is shown in Table 1. At the beginning of this period almost all artifacts were CryptoWall 3.0, but from late October to early November 2015 it shifted to the upgraded CryptoWall 4.0. TeslaCrypt 2.0/2.2 was also detected in small numbers during this period. TeslaCrypt 2.2 in particular continues to spread via email, and for a time attracted a lot of attention in Japan under the name "VVV virus"*47. File formats used in the email attachments included EXE, JS, DOC (Macro), and SCR files, in addition to ZIP archives of these file types. The same applies to Locky, which we will touch upon later. CryptoWall 4.0 subsequently continued to dominate, but in early February 2016 it was replaced by TeslaCrypt 3.0 in an extremely short period of time. Previous versions of TeslaCrypt had an issue with transmitting the symmetric key used to encrypt files to the attacker's server, and it was known that publicly available tools could be used to decrypt the files*48. This issue was fixed in version 3.0. The Locky ransomware detected in early February 2016 was distributed on a massive scale via email at the time*49, but was only detected in limited numbers via websites. TeslaCrypt 4.0 was released around mid-March 2016, and contained bug fixes and some changes from 3.0, including a change where file extensions are no longer added to encrypted files*50. Also, TeslaCrypt announced the cease of development in May 2016 and the master key was made public. Subsequently ESET and other companies have provided decryption tools for versions 3.0 and later*51.

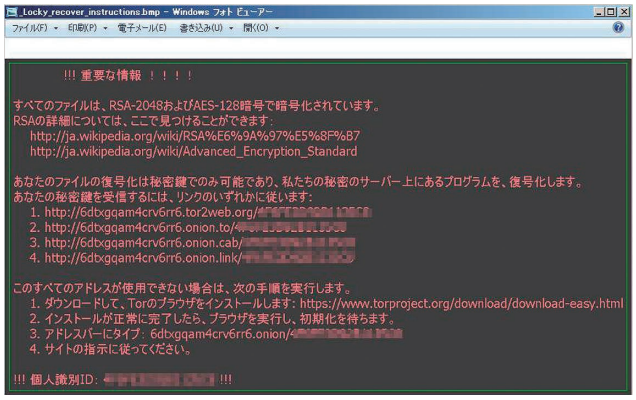


Figure 14: Locky Threat Message

*45 A Trojan called AIDS created in 1989 encrypted file names on the HDD and demanded monetary payment. Refer to SecurityFocus (currently Symantec) column "The Original Anti-Piracy Hack" (http://www.securityfocus.com/columnists/102) for more information.

*46 Refer to the Kaspersky Lab report "Malware Evolution: April June 2005" (https://securelist.com/analysis/malware-evolution-monthly/36052/malware-evolution-april-june-2005/) for more information about the ransomware called gpcode that spread in 2005.

*47 This alias was used due to the extension that was added to the encrypted files. Refer to the Trend Micro blog post "What is the true nature of the 'VVV virus'? 'The influx of CrypTesla ransomware is limited" (http://blog.trendmicro.co.jp/archives/12632) (in Japanese) for more information.

*48 IIJ confirmed that files encrypted with TeslaCrypt 2.0/2.2 could be decrypted using "TeslaCrack" (https://github.com/Googulator/TeslaCrack).

*49 The threat that Locky poses via email was reported on in the Symantec blog post "Locky ransomware on aggressive hunt for victims" (http://www.symantec.com/connect/blogs/locky-ransomware-aggressive-hunt-victims).

*50 Refer to the Bleeping Computer blog post "TeslaCrypt 4.0 Released with Bug Fixes and Stops Adding Extensions" (http://www.bleepingcomputer.com/news/security/teslacrypt-4-0-released-with-bug-fixes-and-stops-adding-extensions/) for more information.

*51 More information available in the ESET blog post, "ESET releases new decryptor for TeslaCrypt ransomware" (http://www.welivesecurity.com/2016/05/18/eset-releases-decryptor-recent-variants-teslacrypt-ransomware/).

■ Flow of Operations

When ransomware such as CryptoWall, TeslaCrypt, or Locky is executed on a victim's computer, files are encrypted and the victim is threatened through the following process:

1. Confirm global IP address
   The ransomware connects to a general IP address confirmation service to check the computer's internet connectivity and global IP address. This process is thought to be preparation to check whether or not the public key can be downloaded. In CryptoWall 3.0, no further processes are executed if this process cannot be performed. Additionally, some variants may use the computer's proxy settings when connecting. CryptoWall 4.0 and TeslaCrypt 3.0/4.0 do not perform this global IP address confirmation.
2. Key exchange with server
   To provide victims who pay the ransom with a way to decrypt files, the attacker needs to have some kind of decryption method on hand (such as on the server that executes the payment process). As detailed later, Locky and CryptoWall use a mechanism that downloads the public key for encryption from a server, so if the connection with this server can be blocked, the processes to follow are not executed. On the other hand, TeslaCrypt has ECDH key parameters embedded in the executable file, so encryption is performed regardless of whether there is a connection with the server.
3. Deletion of VSS control files
   To prevent victims from restoring files using the Volume Shadow Copy Service (VSS) backup function available by default in Windows Vista or later, the VSS control files are deleted. A dialog box is displayed under default settings, but the display will depend on UAC settings. If the ransomware is executed on an account without administrator privileges, this process is not performed.

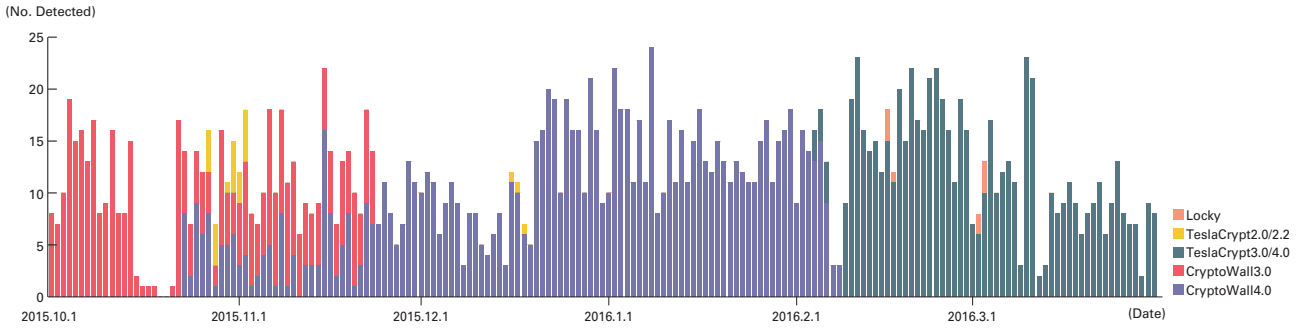


Figure 15: Type and Number of Ransomware Detected by the IIJ MITF Web Crawler (October 1, 2015 to March 31, 2016)

Table 1: Ransomware Detected by the IIJ MITF Web Crawler

	CryptoWall 3.0	CryptoWall 4.0	TeslaCrypt 2.0	TeslaCrypt 2.2	TeslaCrypt 3.0	TeslaCrypt 4.0	Locky
Period of Appearance	January 2015	November 2015	July 2015	December 2015	February 2016	March 2016	February 2016
IP Address Confirmation	Connects to ip-addr.es	None	Connects to ipinfo.io	Connects to myexternalip.com	None	None	None
Proxy Support	Not supported	Supported	Not supported	Supported	Supported	Supported	Not supported
Offline Encryption	Not possible	Not possible	Possible	Possible	Possible	Possible	Not possible
VSS Deletion	Performed	Performed	Performed	Performed	Performed	Performed	Performed
Notes	・Encryption is not performed if the IP address confirmation or server key exchange cannot be performed		・Plagiarizes threat messages of CryptoWall Decryption is ・possible with publicly-available tools	・Also called the VVV virus in Japan ・Decryption is possible with publicly-available tools		・3.0 bugs fixed Stopped adding extensions to encrypted files	・Also tries to reconnect and encrypt network shares that aren't connected

4. Encryption of target files
   Files subject to encryption are selected based on file extensions, etc., and then encrypted with AES using a randomly-generated key, and this symmetric key is embedded in the header of the encrypted files. At this point, the symmetric key is encrypted with ECDH in TeslaCrypt, and RSA in CryptoWall and Locky, to prevent third parties from obtaining it.
5. Display of a threat message
   Various formats of files, such as text, PNG, HTML, etc. are displayed, indicating that content has been encrypted, and showing the procedure to connect to the Web server for payment (Figure 16, Figure 17).
   TeslaCrypt attempts to collect the symmetric key used for encryption by prompting the victim to decrypt an arbitrary file as a trial, and asking the user to upload this file upon accessing the Web server.

■ Handling

If ransomware is executed and content files become unusable, it is extremely difficult to restore (decrypt) them on your own. However, due to the clumsiness of the malware creator, such as in the case of TeslaCrypt mentioned before, or the leak of key information or the ransomware decryptor, there may be rare occasions where effective decryption tools are available. It is necessary to be cautious about the origin and content of such tools, but trying them out is certainly worth consideration.

Unfortunately, in most cases it is not possible to decrypt files on your own, so you are left to make the decision of whether or not to give in to attacker demands. Although it will depend on the occupation or kind of work performed by the victim and the storage policy for content files, the first thing to consider is handling the matter similarly to when there is a storage failure, by performing a clean installation or replacing the equipment. From an organizational perspective, in most cases the file system on individual PCs is probably not all that critical. On the other hand, there are cases where negotiations have taken place with the attackers when the unusable files posed a direct threat to human lives*52. There is no model answer on how to handle such a situation because the importance and value of the files must be considered in addition to business dependencies. However, when opting to give in to the attacker demands, at a minimum, the following two points must be taken into consideration.

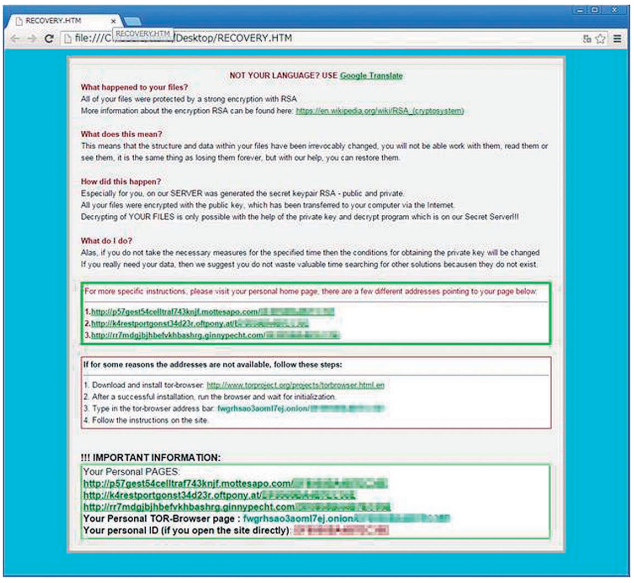


Figure 16: TeslaCrypt 3.0 Threat Message

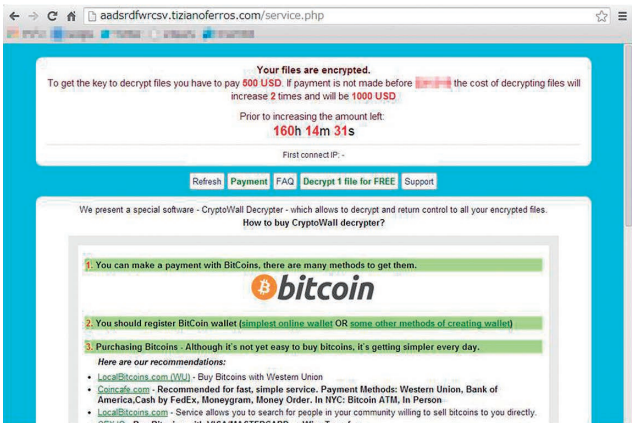


Figure 17: TeslaCrypt 2.2 Screen for Connection to Payment Web Server

*52 A press release by the Hollywood Presbyterian Medical Center (http://hollywoodpresbyterian.com/default/assets/File/20160217%20Memo%20from%20the%20CEO%20v2.pdf) announced they made payment to resume business quickly.

- There is no guarantee that all files will be restored even if payment is made*53
- You will be dealing with people connected to criminal activities (it will be necessary to give a suitable explanation if there is a chance that this fact could become public)

Furthermore, when connecting to the attacker's server, it may indicate that one or several files can be decrypted for free. If a decision is made to test the decryption by sending files, it is necessary to accept the risk that the contents will be leaked to the attackers.

■ Countermeasures

A file system backup is extremely important as a preventative countermeasure in the event of infection. We recommend implementing regular backups of the entire file system or content storage area for individual computers, as well as network drives that can be written to. Because there is a chance that the backup files will also be encrypted, it is necessary to save them in a location where they cannot be accessed by computers that may be infected, such as a directory or drive not configured as a shared directory or drive on the file server. When running client PCs or file servers in a virtual environment, differential backups through snapshots is effective.

Refer to "1.4.2 Hardening Windows Clients Against Malware Infections (Part 1)" for information on malware infection countermeasures on Windows client systems.

1.4.2 Hardening Windows Clients Against Malware Infections (Part 1)

As mentioned in this report under "1.4.1 Various Ransomware and Their Countermeasures," and in previous volumes of IIR, there have been many malware infections through websites that use exploit kits or through email in recent years. In light of this, in this report and the next volume of IIR, we will discuss settings to harden Windows for preventing infections and mitigating the damage caused when malware is received via the aforementioned routes.

■ Requirements

The following applies to Windows 7 SP1 and later for the OS and editions of Professional/Pro and higher. A number of the countermeasures can also be used on Home editions, but there are no implementations of Software Restriction Policies and functions to restrict the execution scope of programs like AppLocker, so we consider this to not be appropriate for business usage, and thus out of scope.

■ Prerequisites

For our descriptions here, we will be using the Local Group Policy Editor in a Windows client that is not part of a domain. Note that these settings and EMET, which will be described later, can be applied to all Windows clients within a domain at the same time, using the Group Policy Management Editor for Windows domains. Note that most screenshots are from the 64-bit version of Windows 10 Enterprise Edition, so there may be minor differences in the items that can be configured depending on the versions of Windows. It is assumed that Windows is installed under C:\ directory.

■ Basics

First, perform software updates to ensure the latest versions are being used.

- Windows Update (including other Microsoft products)
- Web browsers (including third-party browsers such as Firefox and Google Chrome)
- Email clients (including third-party products such as Thunderbird)
- Web browser plug-ins (Flash Player, Adobe Reader, Java)

Any other software being used or software initially installed when the computer was shipped should also be kept up-to-date. It is also a good idea to uninstall any unnecessary or unused software.

*53 The Bleeping Computer blog post "Paying the Coverton Ransomware May Not get your Data Back" (http://www.bleepingcomputer.com/news/security/paying-the-coverton-ransomware-may-not-get-your-data-back/) discusses ransomware called Coverton which fails to decrypt files even if the ransom is paid.

Install anti-virus software and keep it up-to-date, along with keeping up-to-date with the latest definition files. It is also necessary to enable a personal firewall.

■ Do Not Grant Administrator Privileges to Users

The measures introduced in this report assume that policies will be enforced for general users by employing administrator privileges, which prohibits the installation of new programs. However, if users have administrative privileges, they will be able to change policies freely, so only granting user privileges is necessary.

■ Application Whitelisting

Windows and standard Microsoft programs are installed under the C:\Windows or C:\Program Files folders. Most programs prepared by administrators are also installed under either of these folders. Therefore, by prohibiting the execution or loading of programs from folders other than these, you can prevent malware that came as an email attachment or downloaded via drive-by download from being executed or loaded. This technique is called application whitelisting, and its use is recommended by government agencies and other organizations overseas*54. Here, we will cover two methods for applying such restrictions: AppLocker and Software Restriction Policies (SRP).

■ AppLocker

Microsoft added a feature called AppLocker starting with Windows 7. This feature is considered to be a superior version of the Software Restriction Policies (SRP) we will mention later, since it allows more flexible and detailed management. AppLocker can be used on Enterprise editions of Windows 7 or later*55.

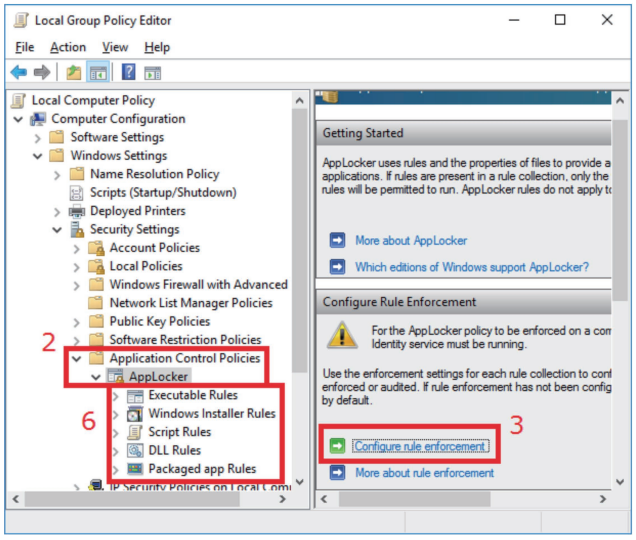


Figure 18: AppLocker Configuration

1. Run the Local Group Policy Editor as an administrator. This can be done by executing gpedit.msc (Figure 18).
2. From the console tree in the left pane, navigate to **Computer Configuration**, **Windows Settings**, **Security Settings**, **Application Control Policies**, **AppLocker** (Figure 18).
3. Click **Configure rule enforcement** in the AppLocker menu displayed in the right pane (Figure 18).
4. In the **AppLocker Properties** dialog box that appears, click the **Advanced** tab, select the **Enable the DLL rule collection** check box, and then click **Apply** (Figure 19).
5. In **AppLocker Properties**, click the **Enforcement** tab, and ensure that the **Configured** check box and **Enforce rules** are selected for all rules. Then click **OK** to close **AppLocker Properties** (Figure 20).
6. Right-click each of the rules under **AppLocker***56, and select **Create Default Rules** (Figure 18).

*54 For example, the NSA in the United States introduces application whitelisting as the first item in their host construction guide for U.S. government agencies. "Host Mitigation Package" (https://www.iad.gov/iad/library/ia-guidance/security-tips/host-mitigation-package.cfm). In addition, a guide for performing application whitelisting using Software Restriction Policies (SRP) has also been published "Application Whitelisting using Software Restriction Policies" (https://www.iad.gov/iad/library/ia-guidance/security-configuration/operating-systems/application-whitelisting-using-srp.cfm).
The Australian Signals Directorate (ASD) stated that 85% of the incidents they responded to within Australian government institutions could have been mitigated using the top 4 strategies. Application whitelisting is the first mitigation strategy listed. AppLocker is also covered in their Implementation Guide. "Strategies to Mitigate Targeted Cyber Intrusions" (http://www.asd.gov.au/infosec/mitigationstrategies.htm).

*55 The directory tree and service control actions for Windows domain policies are slightly different, so replace terms as necessary. For example, in the Windows domain Group Policy Management Editor, navigate to AppLocker via Computer Configuration, Policies, Windows Settings, Security Settings, Application Control Policies, AppLocker. For services, use the same Group Policy Management Editor to navigate to Computer Configuration, Policies, Windows Settings, Security Settings, System Services to display the configuration window for enforcing the automatic launch of services.

*56 In Windows 7, no Packaged app Rules exist.

7. Open the **Services** management window from **Administrative Tools**, etc., and start the **Application Identity** service. Also make sure to switch the **Startup type** to **Automatic**, or the Application Identity service will not start automatically after the next reboot*57.
8. To enable AppLocker, reboot the host you want to enforce policies for, or open a command prompt as an administrator and execute the 'gpupdate /force' command. When attempting to launch an application that is not permitted, a pop-up dialog box such as the one shown in Figure 21 will appear.

Log entries for permission and denial are output to event logs. Open **Event Viewer** and navigate to **Applications and Services Logs**, **Microsoft**, **Windows**, **AppLocker** to view log outputs for each category (Figure 22).

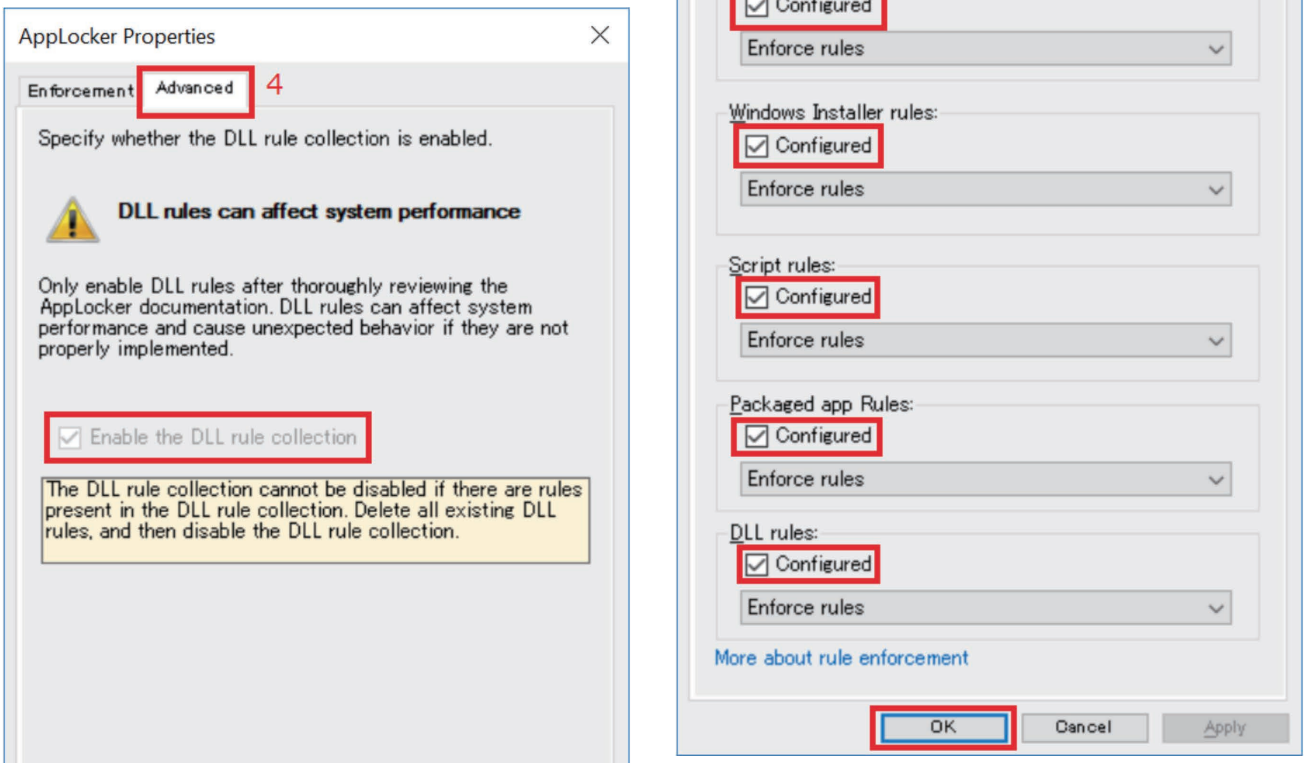


Figure 20: AppLocker Properties (Enforcement)

Figure 19: AppLocker Properties (Advanced)

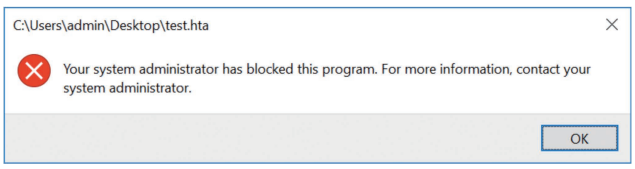


Figure 21: AppLocker - Pop-Up That Appears When a Program is Blocked

*57 In Windows 10 environments, a message saying that access is denied appears even when done as an administrator, and you cannot configure the service to start automatically. If this symptom occurs, we have confirmed that the Startup type will change to Automatic, after a command prompt is opened as an administrator and the following command is executed: sc config appidsvc start=auto.

Software Restriction Policies (SRP)

Due to the fact that AppLocker is included only in the Enterprise edition, we can surmise that Microsoft believes the Enterprise edition should be used in business environments. However, when a pre-installed Windows client PC is purchased for business purposes, most of the time the Pro edition is installed. This makes AppLocker unusable in actual business environments. Furthermore, AppLocker is not available for any edition of a Windows OS prior to Windows 7 (such as Vista). When comparing to AppLocker, there are a number of inconveniences and missing functions. These include the inability to create rules for program types, not logging events where libraries (DLL) are blocked, and not restricting Store apps. Additionally, rules are enforced in user mode instead of kernel mode and policies cannot be imported. Despite these, in most cases applying these restrictions is just as effective as using AppLocker*[58]. For your information, when both Software Restriction Policies and AppLocker are configured on OSes where both are available, the Software Restriction Policy configurations are ignored.

1. Run the Local Group Policy Editor as an administrator. This can be done by executing gpedit.msc (Figure 23).
2. In the console tree in the left pane, navigate to **Computer Configuration**, **Windows Settings**, **Security Settings**, **Software Restriction Policies** (Figure 23).
3. Right-click **Software Restriction Policies**, and then select **New Software Restriction Policies** (Figure 23).
4. Double-click **Enforcement** (Figure 23).
5. In the **Enforcement Properties** dialog box that appears, select **All software files**. Next, select **Enforce certificate rules**, and then click **OK** to close **Enforcement Properties** (Figure 24).
6. Double-click **Designated File Types** to open the **Designated File Types Properties** dialog box (Figure 23).

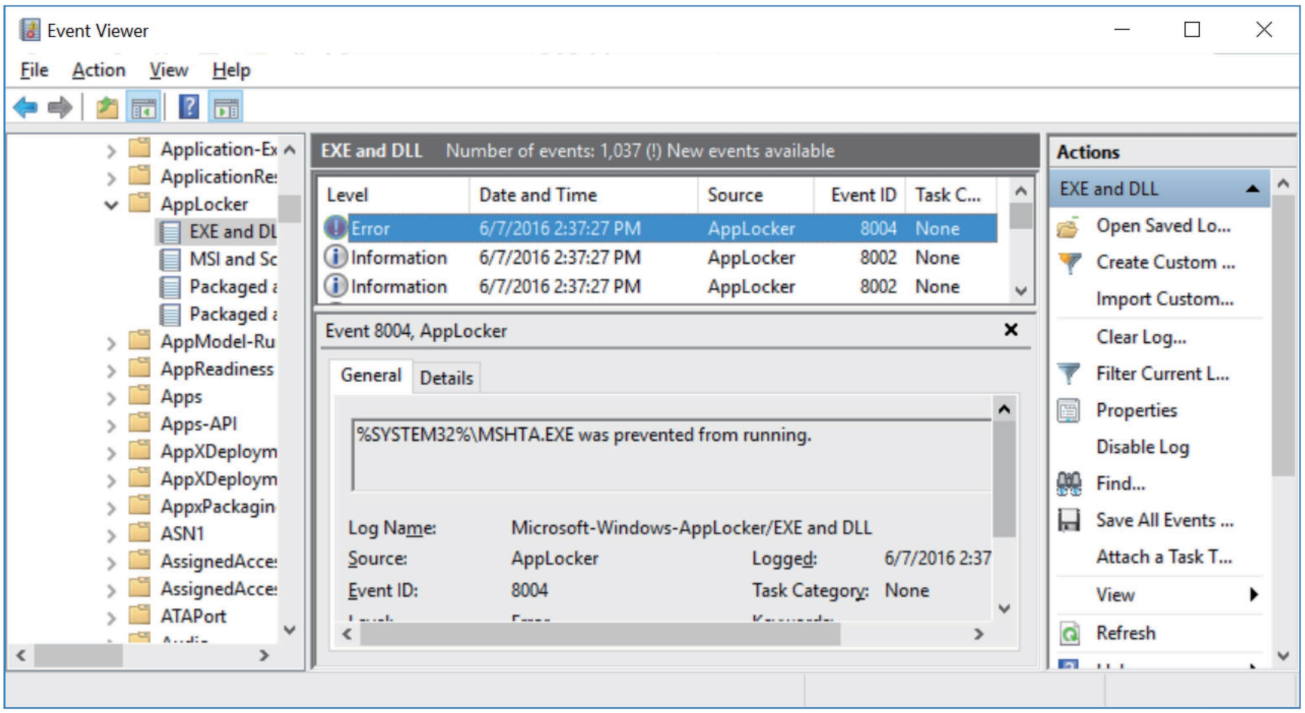


Figure 22: AppLocker - Event Logs

*58 Refer to the following URL for a detailed comparison between AppLocker and Software Restriction Policies. "Use AppLocker and Software Restriction Policies in the Same Domain" (https://technet.microsoft.com/library/hh994614).

7. Select **LNK**, and then click **Remove** (Figure 25). A pop-up dialog box will appear indicating that programs of that type will run with no restrictions. Click **Yes** to close it, and then click **OK** to close **Designated File Types Properties**. Here LNK needs to be removed, or all shortcut files on the desktop and start menu will also be blocked and the computer will become useless, so be sure to remove it from the designated file types. Malicious shortcuts (LNK)*59 that contain VBScript or JScript may present threats, and they are dealt with separately (this will be explained in the next IIR report).
8. Double-click **Security Levels**, and then double-click **Disallowed**.

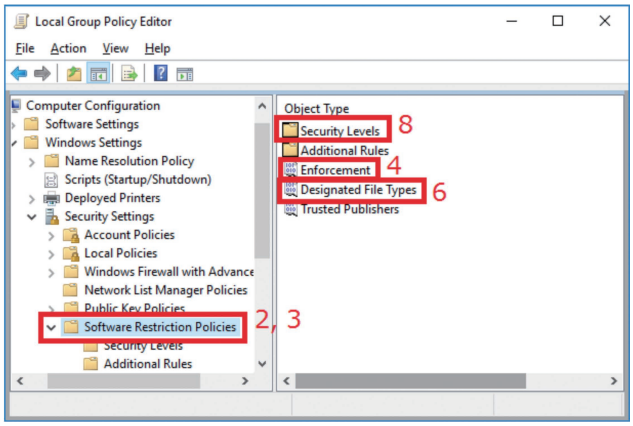


Figure 23: Software Restriction Policies (SRP) Configuration

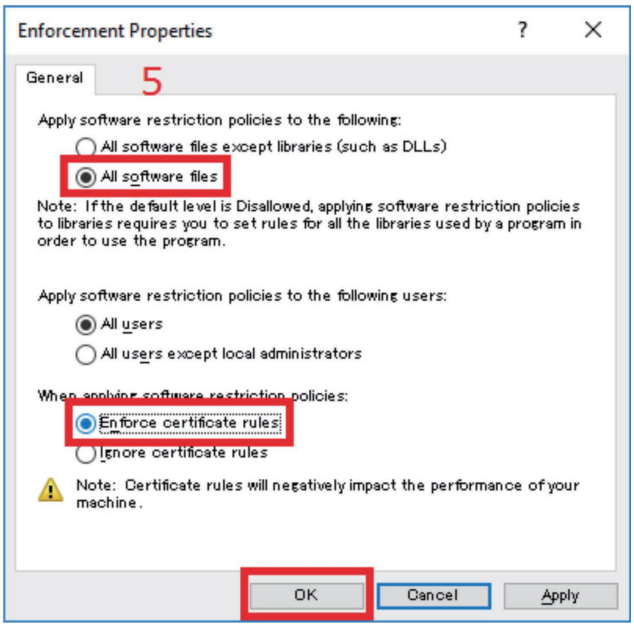


Figure 24: SRP - Enforcement Properties

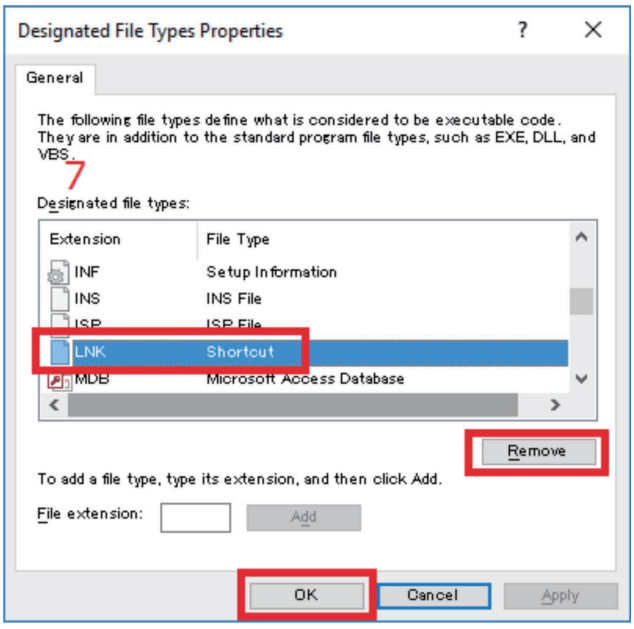


Figure 25: SRP - Designated File Types Properties

*59 The following report provides an example of a technique that involves the execution of VBScript embedded in a LNK file. "Janicab Hides Behind Undocumented LNK Functionality" (https://www.f-secure.com/weblog/archives/00002803.html). There have also been cases of malicious LNK files reported in Japan. For example, in an incident handled by J-CSIP, users were prompted to open a LNK file, which was named to look like a resume. "Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP) Fiscal 2014 Activities Report Supplementary Resource - List of Attack Emails from Attacker 'X'" (https://www.ipa.go.jp/files/000046020.pdf) (in Japanese).

9. In the **Disallowed Properties** dialog box that appears, click **Set as Default** (Figure 26). A pop-up dialog box will appear indicating that some programs may stop working. Click **Yes** to close it. You will then return to the **Disallowed Properties** dialog box. Click **OK** to close it.
10. To enable Software Restriction Policies, reboot the host you want to enforce policies for, or start a command prompt as an administrator and execute the 'gpupdate /force' command.

When the execution of a program is blocked, a pop-up dialog box such as the following will appear, similar to AppLocker (Figure 27).

When blocked, it will be recorded in the event log under Application (Figure 28).

Vulnerabilities That Bypass Restrictions

When malware is run using general user privileges, it will attempt to install the malware under the user directory, so using this function should prevent most malware infections. That said, under default settings a number of vulnerabilities exist. For example, any user is able to save and execute files in the C:\Windows\Temp folder, so if an attacker generates and executes malware there, the default restriction settings will be bypassed. To prevent this from happening, use a tool such as AccessEnum or AccessChk in Sysinternals*60 to investigate whether there are locations where general users can write to under folders where execution is allowed. If there are such locations, you need to add rules to block execution under these folders. There are also a number of additional vulnerabilities reported by researchers*61. If you would like to apply strict restrictions, these vulnerabilities need to be inspected, and rules need to be added accordingly.

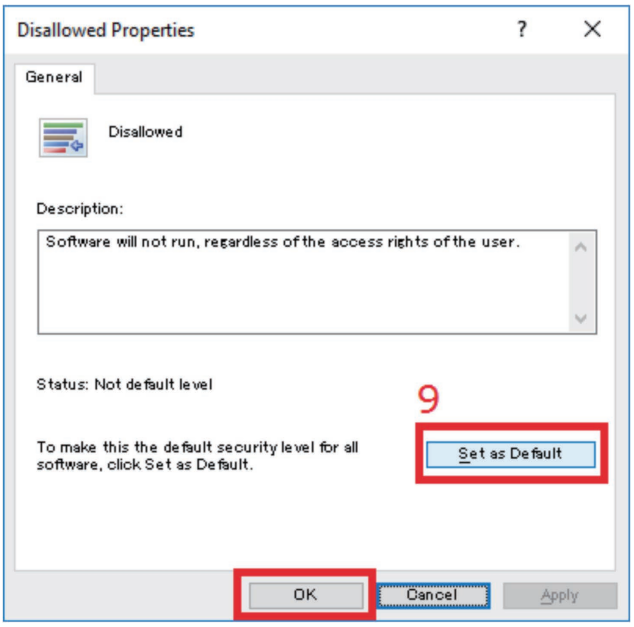


Figure 26: SRP - Disallowed Properties

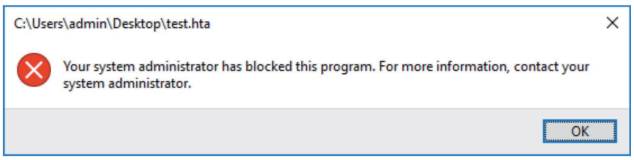


Figure 27: SRP - Pop-Up That Appears When a Program is Blocked

*60 AccessEnum (https://technet.microsoft.com/en-us/sysinternals/bb897332). AccessChk (https://technet.microsoft.com/en-us/sysinternals/bb664922).

*61 For example, a number of techniques for bypassing AppLocker restrictions and their corresponding countermeasures are discussed in the following URLs. "Protecting Windows Networks - AppLocker" (https://dfir-blog.com/2016/01/03/protecting-windows-networks-applocker/). "Application Whitelist Bypass Techniques" (https://github.com/subTee/ApplicationWhitelistBypassTechniques). Additionally, the following URL explains a technique for remotely downloading and executing script using regsvr32.exe. "Bypass Application Whitelisting Script Protections - Regsvr32.exe & COM Scriptlets (.sct files)" (http://subt0x10.blogspot.com/2016/04/bypass-application-whitelisting-script.html).

The WinSxS Folder

The WinSxS folder stores Windows Update backups as well as a variety of Windows functions (PowerShell, .Net Framework, Hyper-V, etc.). When these functions are enabled, hard links to files in this folder are created in the System32 folder, etc., so they are available to users without having to worry about the path. However, even before they are enabled, it is possible to execute the programs directly from the WinSxS folder. For example, PowerShell and rundll32.exe exist in this folder, so to prevent exploitation, it is necessary to block them. Some people may believe that restricting the execution and loading of all files in the WinSxS folder will achieve this. However, we have learned through our investigations that some components directly load libraries found under the WinSxS folder.

With AppLocker, it is possible to manage rules for executable files (EXE) and libraries (DLL) separately, so it is possible to block all executable files while leaving libraries unblocked, or block all files and when an issue arises with a library, check the logs and add them. On the other hand, Software Restriction Policies cannot be configured by program type, so the only option is to block the entire WinSxS folder, and then only allow programs as problems arise. However, when determining what to allow, libraries (DLL) that are blocked are not logged when using Software Restrictions Policies, so it is not easy to determine what to allow. This issue can be prevented by using Sysmon, Process Monitor, and Process Explorer*62, etc. in Sysinternals with WinSxS enabled during testing to record the events when libraries are loaded, and then adding them as rules to be allowed.

Restricting Administrator Privileges

The default rules for AppLocker do not restrict users belonging to the Administrators group. It is possible to apply restrictions similar to general users by removing these rules. By default, Software Restriction Policies apply to all users (Figure 24).

(To be continued in the next report)

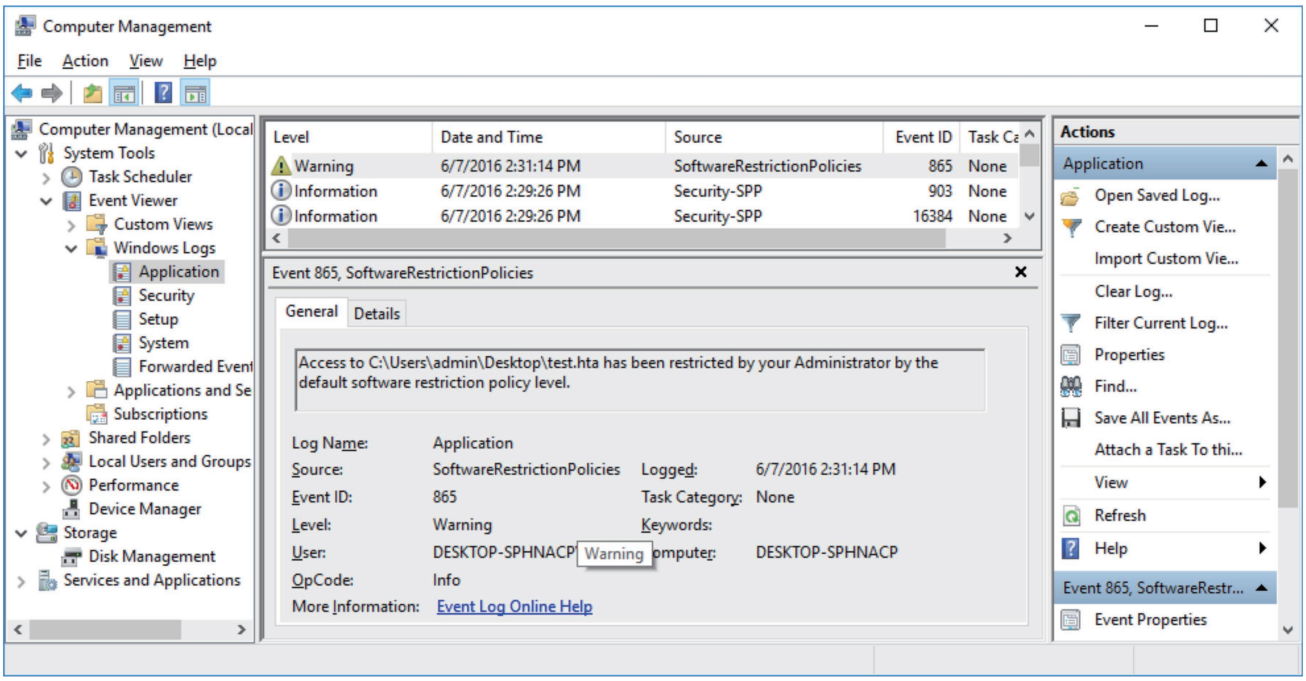


Figure 28: SRP - Event Logs

*62 Sysmon (https://technet.microsoft.com/en-us/sysinternals/sysmon). Process Monitor (https://technet.microsoft.com/en-us/sysinternals/bb896645). Process Explorer (https://technet.microsoft.com/en-us/sysinternals/bb896653.aspx).

1.4.3 Trends in Post-Quantum Cryptography

In February 2016, the PQCrypto2016 (Post-Quantum Cryptography 2016)*63 international conference on post-quantum cryptography was held in Fukuoka City. On the first day of this conference, the National Institute of Standards and Technology (NIST), which develops standards documents related to information security in the United States, announced they will hold a post-quantum cryptography competition*64. As a result, a wide range of interested parties participated, including researchers interested in NIST trends going forward, and vendors looking to determine a direction for future product lineups. Over 200 individuals from Japan and overseas attended the conference, an extraordinary number for an international conference of this scale. Aside from this announcement from NIST, research in this area is becoming more active, including the launch of a project last year in Europe where considerable research funds are being spent. In this report we discuss the technical background of post-quantum cryptography, and take a look at some future trends.

■ The Impact of the Advent of Quantum Computers on Cryptographic Technology

Post-quantum cryptography*65 is a concept proposed by Professor Daniel J. Bernstein in 2003. It is a general term used to describe cryptographic algorithms that, taking the appearance of quantum computers into account, aim to replace the cryptographic technology currently used. In addition to post-quantum cryptography, terms such as quantum safe cryptography and quantum resistant cryptography are also used, but these all refer to the same concept.

The RSA and (EC)DH cryptographic algorithms that are currently widely used as public key cryptosystems provide security based on the difficulty of prime factorization and the complexity of the discrete logarithm problem, respectively. These two problems are known to be extremely difficult to solve using current computer architecture. In contrast, Shor's algorithm*66 proposed in 1994 shows that these two problems can be solved in polynomial time using quantum computers*67. This means that public-key cryptographic algorithms currently in mainstream use will be threatened by the advent of quantum computers.

Let us examine just how useless current cryptographic algorithms will become. It is possible to explain this using an indicator called bits of security*68. The expression "n bits of security" is used as a concept to indicate the strength of a cryptographic algorithm and the progress toward its compromise. The parameter n indicates that the number of computations required to attack corresponding algorithm is 2^n (2 to the n-th power). In symmetric-key cryptography, this 2^n (where n is the symmetric key length in bits) corresponds to the size of the entire key space. For hash functions, when the output length is n bits, the theoretical number of necessary computations is 2^n for preimage resistance, and $2^{n/2}$ for collision resistance.

In general, it is necessary to gradually transition to newer cryptographic algorithms. SP 800-131A, which indicates NIST's algorithm transition plan, was revised in November 2015 to disallow algorithms that have less than 112 bits of security*69. The symmetric key cryptographic algorithm Two-key Triple-DES (which uses 112-bit keys, but attack techniques that are more

*63 The Seventh International Conference on Post-Quantum Cryptography (https://pqcrypto2016.jp/). A two-day lecture titled Winter School (https://www.youtube.com/playlist?list=PLCAbx7kHwCGKLMt1-geJmx9QmOCvXLRdz) and footage of the conference (https://www.youtube.com/playlist?list=PLCAbx7kHwCGLPpgETzBqQg11comaFCF_H) have been posted online.

*64 The following presentations were given at the PQCrypto2016 conference. Dustin Moody, "Post-Quantum Cryptography: NIST's Plan for the Future" (https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf).

*65 Daniel J. Bernstein, "A brief survey of post-quantum cryptography", PQCrypto2008 invited lecture, 2008 (http://cr.yp.to/talks/2008.10.18/slides.pdf).

*66 Peter W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", 35th Annual Symposium on Foundations of Computer Science (FOCS), 1994 (https://www.computer.org/csdl/proceedings/focs/1994/6580/00/0365700.pdf). The current record for prime factorization is 56153, which was disclosed in November 2014 (http://arxiv.org/abs/1411.6758).

*67 Jason LeGrow, "Post-Quantum Security of Authenticated Key Establishment Protocols", A thesis presented to the University of Waterloo, 2016 (https://uwspace.uwaterloo.ca/bitstream/handle/10012/10386/LeGrow_Jason.pdf).

*68 Examples of the compromise of cryptographic algorithms, as well as explanations of bits of security and equivalent security, are provided in Vol.8 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol08_EN.pdf) under "1.4.1 Trends in the Year 2010 Issues on Cryptographic Algorithms".

*69 National Institute of Standards and Technology (NIST), "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", NIST Special Publication 800-131A, 2015 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf).

efficient than brute force exist) was removed. Only key lengths of 112 bits or longer are acceptable for use in MAC (Message Authentication Codes) such as HMAC, and only SHA-2 or SHA-3 can be used as the hash functionsfor creating signatures, replacing the already compromised SHA-1*70.

Also, by estimating the number of computations necessary for attacks on public key cryptosystems, key lengths with n bits of security have been determined for each algorithm. One example of this is SP 800-57 by NIST, which was revised in January 2016*71. 112 bits of security is valid until 2030, and beyond that, there is expected to be a shift to algorithms with 128 bits of security. Public keys with security equivalent to 112 bits include RSA-2048, DSA-2048, ECDSA-224, and ECDH-224, so the use of shorter key lengths than these has already been prohibited, and after 2031 a transition to algorithms such as RSA-3072 and ECDH-256 should take place.

However, if quantum computers make an appearance, these assumptions will collapse. One indicator of this is Grover's algorithm*72, which was presented in 1996. By using Grover's algorithm, it was shown that for a cryptographic algorithm with n bits of security based on current computer architecture, it is only possible to guarantee n/2 bits of security based on the computing ability of quantum computers. For example, this means the AES-128 symmetric key cryptography that is currently used would only provide 64 bits of security. As a result, to ensure 128 bits of security it would be necessary to shift to AES-256, which uses a 256 bit key. Similarly, for hash functions, when considering a case where SHA-256 is used for signing, this only provides 64 bits of security for ensuring collision resistance. Thus to ensure at least 128 bits of security, algorithms with an output length of 512 bits or higher, such as SHA-512 or SHA3-512 need to be used.

The same applies to public key cryptosystems, so key lengths currently believed to have 256 bits of security need to be used to ensure 128 bits of security. According to the aforementioned SP800-57, this corresponds to RSA-15360 or ECDH-512. Furthermore, a report published by ETSI (European Telecommunications Standards Institute) in June 2015 presented an even grimmer outlook*73, stating that even when key lengths currently believed to provide 256 bits of security are used, such as those mentioned above, they will actually provide 0 bits of security.

■ Searching for Cryptographic Algorithms with New Basis for Security

In light of the background above, there is growing demand for public key cryptographic algorithms with a security basis that is different than previous systems. Starting with developments in academia, the PQCrypto international conference has been held about every 18 months since 2006*74, with the aforementioned PQCrypto2016 being the 7th to date. Since 2013, ETSI has jointly held the IQC/ETSI Quantum-Safe Crypto Workshop*75 with IQC (Institute for Quantum Computing). At the October 2015 conference, a consensus was reached regarding the need to standardize post-quantum cryptography*76. The 4th workshop is scheduled for September 2016, so we expect information will be shared on an ongoing basis.

Similarly, in Europe there is the H2020 PQCRYPTO project. H2020 (Horizon 2020)*77 is a pioneering, Europe-wide research support program through EU funding that is said to be the successor to FP7, which supported both the ECRYPT (European Network of Excellence in Cryptology) and ECRYPT2 programs. The H2020 PQCRYPTO project*78 was launched in March 2015 and will be

*70 However, signature algorithms with less than 112 bits of security and SHA-1 are permitted for legacy use in signature verification. Additionally, these restrictions do not apply SHA-1 usage for purposes not related to signature generation or verification, which is considered acceptable. Because SHA-1 has more than 112 bits of preimage resistance, note that HMAC-SHA-1 is not vulnerable. Furthermore, SHA-2 and SHA-3 each have 224, 256, 384, and 512 bit variations for the digest output length.

*71 National Institute of Standards and Technology (NIST), "Recommendation for Key Management, Part 1: General", NIST Special Publication 800-57 Part 1 Revision 4, 2016 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf).

*72 Lov K. Grover, "A fast quantum mechanical algorithm for database search", 28th Annual ACM Symposium on the Theory of Computing (STOC), 1996 (http://arxiv.org/abs/quant-ph/9605043).

*73 European Telecommunications Standards Institute (ETSI), "Quantum Safe Cryptography and Security", ETSI White Paper No. 8, 2015 (http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf).

*74 PQCrypto2006: International Workshop on Post-Quantum Cryptography (http://postquantum.cr.yp.to/).

*75 European Telecommunications Standards Institute (ETSI), 3rd ETSI/IQC Workshop on Quantum-Safe Cryptography (http://www.etsi.org/news-events/events/949-etsi-iqc-3).

*76 European Telecommunications Standards Institute (ETSI), "ETSI workshop confirms need to accelerate on Quantum-Safe Cryptography standards" (http://www.etsi.org/index.php/news-events/news/1013-2015-10-news-etsi-workshop-confirms-need-to-accelerate-on-quantum-safe-cryptography-standards).

*77 European Commission, Horizon 2020 (http://ec.europa.eu/programmes/horizon2020/).

*78 PQCRYPTO (Post-Quantum Cryptography for Long-Term Security) project (https://pqcrypto.eu.org/).

active over a three year time period, to carry out research activities related to post-quantum cryptology. By September 2015, six months after its activities began, a tentative list (portfolio) of recommended post-quantum cryptographic algorithms had already been put together*79.

Meanwhile, ahead of NIST's February 2016 announcement in the United States, in April 2015 a NIST-led workshop was held in conjunction with PKC2015*80. In August 2015, a request to stop referring to the Suite B cryptography list*81 used for U.S. government procurement was sent out, in particular for the new implementation of devices or systems. Additionally, prior to PQCrypto2016, public comments*82 were solicited with a March deadline, and in April the first edition titled, NISTIR 8105*83 was released. According to the February announcement, it is expected that documentation will be created between 2023 and 2025, and technical verification will be performed with the following timeline. The overview of an official competition will be announced around the fall of 2016, the deadline for entries will be November 2017, and a workshop centering on the presentations by the entrants will be held in early 2018. Following this, standardization is expected to take place within three to five years after technical analysis. It has been indicated that a proper standardization approach will be taken as opposed to narrowing down to a single algorithm as with the AES and SHA-3 competitions, or presenting a portfolio like NESSIE*84.

Table 2: Post-Quantum Cryptography Classifications

Type	Overview	Cryptanalytic Challenge
Lattice-based cryptography	When an n-dimensional real space and one of its bases are given, a vector space consisting of all linear combinations of the basis with integer coefficients is called a lattice. A lattice with a given basis can be represented with a different basis. The Shortest Vector Problem (SVP) for a lattice is considered to be difficult to solve as n becomes larger. Lattice-based cryptography is public key cryptography constructed based on this difficulty. NTRU is one of the algorithms that has been invented for practical use. Besides SVP, other problems such as Learning with Errors (LWE) have been proposed, and this is one of the research areas that have been actively studied in recent years.	TU Darmstadt Lattice Challenge*85
Code-based cryptography	A public key cryptographic system whose security is based on what is known to be a NP-hard problem, the maximum-likelihood decoding problem for a randomly provided linear code. The McEliece algorithm published in 1978 uses Goppa codes with the parameters n=1024, k=524, and t=50. However, its security is estimated to be around 60 bits, and it has the disadvantage of requiring a very long public key to ensure sufficient security.	Cryptanalytic challenges for wild McEliece*86
Multivariate polynomial cryptography	It is said that the origin of this series of primitives is the Matsumoto-Imai algorithm, a multivariate quadratic public key cryptosystem presented at EUROCRYPT 1988. To generalize the original idea, consider n-variate polynomials over a finite field of order q. In this case, it is believed that solving a system of equations is difficult when n is sufficiently large and the public key algorithm is based on this difficulty. However, efficient attack methods against this are known, such as ones using Gröbner bases.	Fukuoka MQ Challenge*87
Hash-based signatures	A digital signature scheme where leaves of a binary tree are considered as the data to be signed and the root of the tree is generated and signed by repeating a hash chain to make the whole tree form a Merkle tree. Because the scheme uses a preimage resistant cryptographic hash function, computing the preimage for any hash value is difficult, and thus it is considered to be difficult to alter the whole tree. Currently, the CFRG is developing a standard called XMSS, and there are also other schemes such as SPHINCS, which was presented at EUROCRYPT last year.	

*79 PQCRYPTO project, "Initial recommendations of long-term secure post-quantum systems", 2015 (https://pqcrypto.eu.org/docs/initial-recommendations.pdf).

*80 National Institute of Standards and Technology (NIST), Workshop on Cybersecurity in a Post-Quantum World (http://www.nist.gov/itl/csd/ct/post-quantum-crypto-workshop-2015.cfm).

*81 The Information Assurance Directorate (IAD), Commercial National Security Algorithm Suite (https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm).

*82 National Institute of Standards and Technology (NIST), "Public Comments Received on NISTIR 8105 - Draft Report on Post-Quantum Cryptograph", 2016 (http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/nistir-8105/nistir-8105-public-comments-mar2016.pdf).

*83 National Institute of Standards and Technology (NIST), "Report on Post-Quantum Cryptography", NISTIR 8105, 2016 (http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf), "NIST Kicks Off Effort to Defend Encrypted Data from Quantum Computer Threat", 2016 (http://www.nist.gov/itl/csd/nist-kicks-off-effort-to-defend-encrypted-data-from-quantum-computer-threat.cfm).

*84 NESSIE (New European Schemes for Signatures, Integrity, and Encryption) consortium, "Portfolio of recommended cryptographic primitives" (https://www.cosic.esat.kuleuven.be/nessie/deliverables/decision-final.pdf).

*85 TU Darmstadt Lattice Challenge (https://latticechallenge.org/). SVP (Shortest Vector Problem) Challenge (https://latticechallenge.org/svp-challenge/index.php). Ideal Lattice Challenge (https://latticechallenge.org/ideallattice-challenge/index.php).

*86 Cryptanalytic challenges for wild McEliece (https://pqcrypto.org/wild-challenges.html).

*87 Fukuoka MQ Challenge (https://www.mqchallenge.org/). Takanori Yasuda et al., "MQ Challenge: Hardness Evaluation of Solving Multivariate Quadratic Problems" (https://eprint.iacr.org/2015/275).

■ Strong Candidates for Post-Quantum Cryptographic Algorithms

The four post-quantum cryptographic systems currently expected to be used are shown in Table 2. It is anticipated that these will not be broken even if quantum computers appear.

Of these systems, the aforementioned H2020 PQCRYPTO project portfolio lists code-based cryptography and hash-based signatures. Meanwhile, in Japan the cryptanalysis of lattice-based cryptography*88 is being actively researched, and a competition originating in Japan is being held for multivariate polynomial cryptography. Furthermore, at the IETF the CFRG (Crypto Forum Research Group)*89 is discussing post-quantum cryptography, and drafting of XMSS (Extended Hash-Based Signatures)*90, a type of hash-based signatures, is ongoing. Efforts to gather opinions from the cryptographic community also continued at the interim meeting*91 during EUROCRYPT2016, which was held in May 2016. Discussions regarding post-quantum cryptography also took place at the CFRG meeting at IETF-95 held in April 2016*92.

As you can see from the NIST standardization schedule, the transition to post-quantum cryptography is not an urgent matter, but it is best to consider it within a mid- to long-term perspective. Since these cryptographic methods have a new basis for security, it is first necessary to estimate how strong they actually are. Therefore, the various competitions shown in Table 2 are being held to further research into more efficient attack methods. Meanwhile, besides these computationally secure methods based on trapdoor functions, which allow decryption only by a secret key chosen from a certain key space, research is also being performed on information-theoretically secure methodse*93. For each alternative, it is necessary to transition slowly while taking operational costs and practicality into account, and there will likely be a need to keep up to date with future trends.

1.5 Conclusion

This report has provided a summary of security incidents that IIJ has responded to. In this report we discussed various ransomware and their countermeasures, and examined hardening Windows clients against malware infections (part 1). We also looked at trends in post-quantum cryptography. IIJ makes every effort to inform the public about the dangers of Internet usage by identifying and disclosing information on incidents and associated responses through reports such as this.

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

Masafumi Negishi (1.2 Incident Summary)
Tadashi Kobayashi, Tadaaki Nagao, Hiroshi Suzuki, Minoru Kobayashi, Hisao Nashiwa (1.3 Incident Survey)
Hisao Nashiwa (1.4.1 Various Ransomware and Their Countermeasures)
Hiroshi Suzuki (1.4.2 Hardening Windows Clients Against Malware Infections (Part 1))
Yuji Suga (1.4.3 Trends in Post-Quantum Cryptography)
Office of Emergency Response and Clearinghouse for Security Information, Advanced Security Division, IIJ

Contributors:
Yasunari Momoi, Hiroyuki Hiramatsu, Office of Emergency Response and Clearinghouse for Security Information, Advanced Security Division, IIJ

*88 Seito et al., "The latest trends in 'lattice-based cryptography' algorithms that can withstand quantum computer attacks", Discussion Paper Series 2015-J-9, 2015 (http://www.imes.boj.or.jp/research/abstracts/japanese/15-J-09.html) (in Japanese). Yoshinori Aono et al., "Improved Progressive BKZ Algorithms and their Precise Cost Estimation by Sharp Simulator" (https://eprint.iacr.org/2016/146).
*89 IETF Datatracker, Crypto Forum (https://datatracker.ietf.org/rg/cfrg/documents/).
*90 Andreas Huelsing et al., "XMSS: Extended Hash-Based Signatures" (https://datatracker.ietf.org/doc/draft-irtf-cfrg-xmss-hash-based-signatures/).
*91 Agenda of interim meeting at EuroCrypt2016 (https://www.ietf.org/proceedings/interim/2016/05/12/cfrg/agenda/agenda-interim-2016-cfrg-1).
*92 IETF95 CFRG meeting, "Post Quantum Secure Cryptography Discussion" (https://www.ietf.org/proceedings/95/slides/slides-95-cfrg-4.pdf).
*93 Junji Shikata, "Trends and Development of Information-Theoretic Cryptography", IEICE Transactions 98-A (1), 2015 (http://search.ieice.org/bin/summary.php?id=e98-a_1_16).

The Latest Trends in Spam

2.1 Introduction

In the first IIR Messaging Technology article in a year, we will report on technical information about email, including trends in spam and spam countermeasures. There has been a downward trend in the volume of spam over the past few years, but recently there was a temporary spike in March 2016. In this report we discuss the results of our investigation into the regions from which this increase originated. Regarding trends in email technologies, we discuss our findings regarding the adoption status of sender authentication technology that it is hoped will become more widespread in the future, with a focus on DMARC.

2.2 Spam Trends

In this section we look at changes in spam trends, based on trends in the ratios of spam detected by the spam filter provided through IIJ's email services. As we have done up until now, trends in the ratio of incoming mail determined to be spam relative to the overall volume of incoming mail collated by week are shown using graphs and other means. For some time the volume and ratio of spam had dropped to significantly lower levels than 2008 when the IIR was first published, but there was a temporary rise in March 2016.

The graph in Figure 1 that indicates spam ratio trends incorporates three years' worth of data, including the year since the last IIR report (Vol.27), covering the 53 weeks between March 30, 2015, and April 3, 2016. See IIR Vol.27 for information about trends previous to this. As you can see in the graph, the ratio of spam has generally been decreasing except for long holiday periods such as the year-end and New Year holidays. However, since around 2015 the range of reduction has narrowed. The average ratio for fiscal 2015 was 24.2%. The ratio in fiscal 2014 was 31.7%, so this represents a drop of about 7.5%. The decrease from fiscal 2013 to fiscal 2014 was 15.7%. However, in March 2016 the rate once again began to trend upward, rising to as high as 44.8% in the week of March 28, 2016. Following this, preliminary figures indicated a drop back to around 20%, so we believe this was a temporary spike. We will analyze trends for the increase in spam during this period a little later.

2.2.1 Risk Remains High

According to a report published by the National Police Agency on March 17, 2016*1, the total monetary damage caused by illegal remittances related to Internet banking in 2015 exceeded the record high of the previous year, coming to approximately 3,073,000,000 yen. There was also a record 3,823 incidents of targeted email attacks reported by affiliated business operators, so the risk associated with email remains high. Reports also indicate that in 77% of cases most sender addresses in targeted emails were spoofed, so it is clear there is an urgent need to popularize and implement sender authentication technology to protect against the spoofing of sender information.

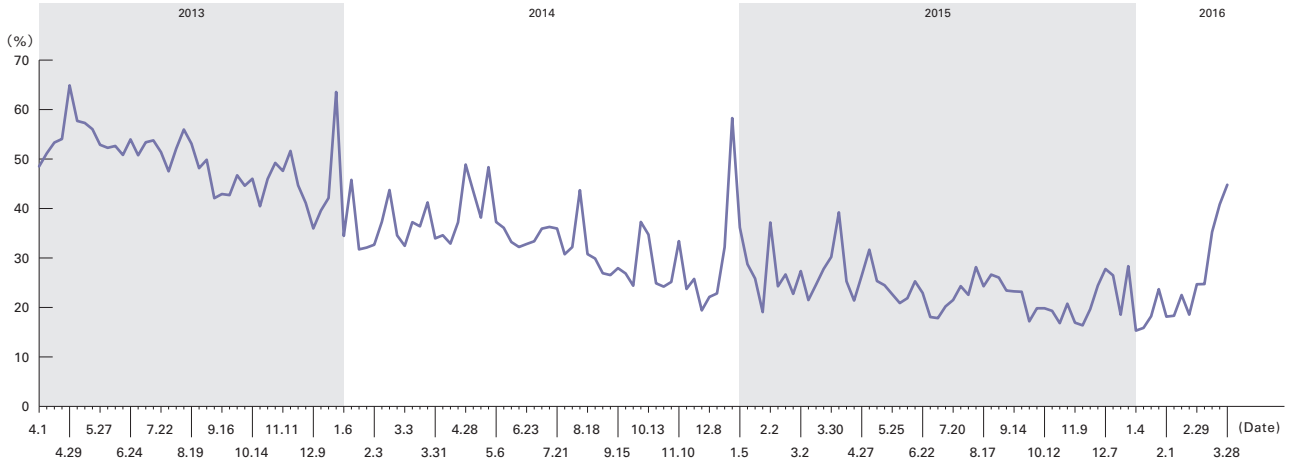


Figure 1: Spam Ratio Trends

*1 Report on Cyberspace Threats for 2015 (http://www.npa.go.jp/kanbou/cybersecurity/H27_jousei.pdf) (in Japanese).

2.2.2 Ratios for Regional Sources of Spam

The graph in Figure 2 shows sources of spam by region between January and March 2016, which corresponds to the fourth quarter of fiscal 2015.

During this period, the region from which most spam originated was the United States (US), at 16.8%. Among the surveys we have presented to date, this is the first time since IIR Vol.10 (third quarter of 2010) that the United States has been the top regional source. After holding the top position up until now, China (CN) fell to second place at 6.4%. Brazil (BR) was the third highest regional source, and also had a ratio of 6.4%. Fourth place was Japan (JP), which once again had a ratio of 6.4%. Following on from that in order was India (IN, 6.3%), Vietnam (VN, 6.1%), Mexico (MX, 5.4%), Hong Kong (HK, 3.1%), Argentina (AR, 2.5%), and Spain (ES, 2.5%). Other than Hong Kong and Vietnam, which are close to Japan, we can see that regions with large territories and high populations held the top positions. Figure 3 shows trends in the volume of spam for these top 10 countries. This time we examine trends in spam volumes rather than the ratio of spam, to analyze the spam increase in March 2016. For that reason no figures are shown on the vertical axis, but a clear comparison can be made between each region.

2.2.3 Trends in the Major Regional Sources

As you can see from Figure 3, among the top regions the United States (US), China (CN), Japan (JP), and Hong Kong (HK) were high in the rankings from the beginning, but in the March 2016 period when the volume of spam spiked they did not increase much. During this period, the peak volume of spam sent from these countries was two to three times that of the lowest volume. Meanwhile, in the other top regions of India (IN), Vietnam (VN), Mexico (MX), Brazil (BR), Argentina (AR), and Spain (ES), the peak volume was at least 10 times the minimum, and in the case of Argentina it was 85 times higher. As each of these regions saw an increase in March 2016 when the ratio of spam was high, we know they contributed to the rise in spam during this period. Because these regions are geographically dispersed, we speculate that the spike may have been caused by a botnet sending spam actively. We believe there is an ongoing need to take measures against botnets like this through international cooperation.

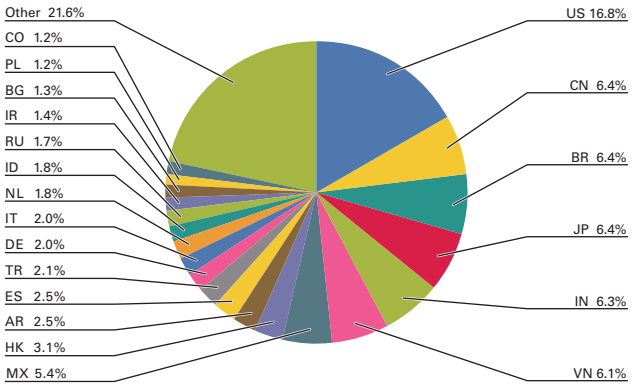


Figure 2: Ratios for Regional Sources of Spam

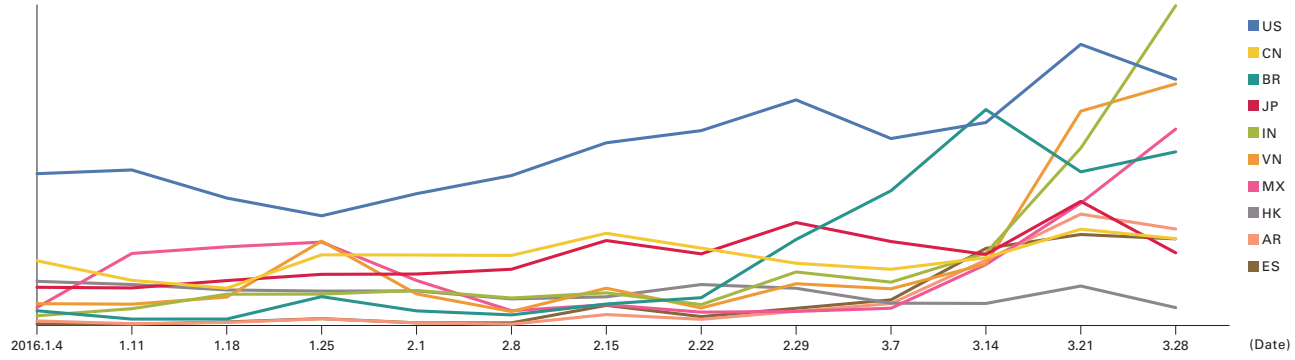


Figure 3: Trends in the Top 10 Regional Sources of Spam

2.3 Trends in Email Technologies

Here we will report on the adoption status and technological trends regarding the sender authentication technology that is also an effective spam countermeasure, with a particular focus on DMARC*2.

We have previously discussed technical details and adoption trends for the SPF*3 and DKIM*4 sender authentication technologies, but in the future we feel that the DMARC standard based on these two technologies will become the main technology used.

2.3.1 An Overview of DMARC

We have already discussed DMARC a number of times since IIR Vol.15, but here we will once again give a summary of its features. DMARC is also a type of sender authentication technology for verifying whether or not the domain used is a legitimate sender based on the sender information. Its main characteristics are as follows.

- Based on matching the domain authenticated using SPF or DKIM with From (RFC5322.From) in the email header (or verifying that the organization is the same)
- Enables recipient behavior to be indicated via policies when sender (domain management) authentication fails
- Senders can specify the report destination when authentication fails
- This information is expressed using a DNS TXT resource record

In other words, DMARC is technology that uses the authentication results of SPF and DKIM, which are either already in widespread use or becoming more prevalent. When DMARC authentication passes, it means the sender information (RFC5322.From) in the header that can be referenced by the email recipient also matches. The sender can confirm that email was sent over the correct route because they receive information in report form when authentication fails. Previously, domains that could be authenticated using SPF or DKIM did not always provide sender information that was easy for the ultimate email recipient to confirm. In a sense, using DMARC authentication has made it possible to unify the domains to be authenticated, making this clearer for the recipient as well.

2.3.2 DMARC Adoption Status

IIJ's email services have supported DMARC since 2014, and incoming mail is authenticated using DMARC. Figure 4 shows DMARC-based authentication result ratios for the three-month period from January to March 2016. Figure 5 and Figure 6 show authentication result ratios for SPF and DKIM, which DMARC authentication is based on, over the same period.

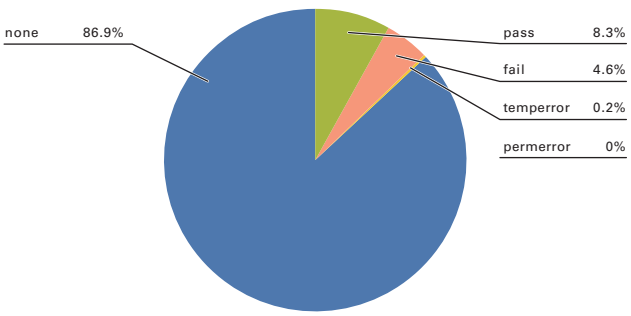


Figure 4: DMARC Authentication Result Ratios for Incoming Mail

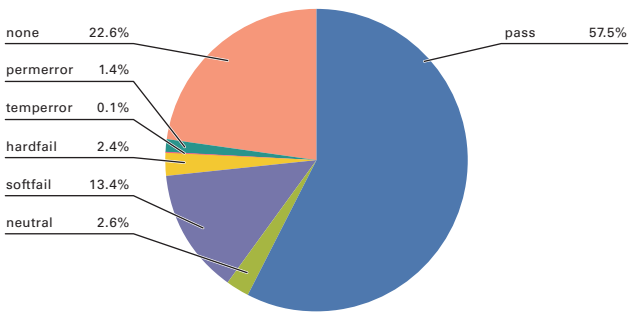


Figure 5: SPF Authentication Result Ratios for Incoming Mail

*2 Domain-based Message Authentication, Reporting, and Conformance (DMARC), RFC7489 (https://rfc-editor.org/rfc/rfc7489.txt).
*3 Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1, RFC7208 (https://www.rfc-editor.org/rfc/rfc7208.txt).
*4 DomainKeys Identified Mail (DKIM) Signatures, STD76, RFC6376 (https://www.rfc-editor.org/rfc/rfc6376.txt).

First, looking at the SPF authentication result ratios in Figure 5, by excluding "none" results that mean SPF authentication could not be performed, we can see that this time a total ratio of 77.4% of senders have implemented SPF. The last time authentication results were presented was in IIR Vol.23 in 2014, and since then this ratio has increased by 4.2%. Because it is comparatively easy for senders to implement SPF, the implementation ratio for SPF has so far tended to be high, and we can see that in this survey the ratio is still increasing slowly.

In the authentication ratios for DKIM in Figure 6, the total for implementation ratios other than "none" came to 20.1%. This was again an 8.5% increase over last time. That means even though the implementation ratio was originally low for DKIM, as it costs quite a bit for senders to deploy, we can see that these ratios are also gradually climbing. The implementation of SPF or DKIM is a prerequisite for implementing DMARC, and as shown in Figure 4, the implementation ratios for DMARC other than "none" results that indicate DMARC authentication is not possible came to 13.1%. Once SPF and DKIM are adopted, DMARC can be implemented by simply adding a DMARC record to the TXT resource record for the "_dmarc" subdomain. In light of this, we believe the implementation ratio for DMARC is lower than SPF and DKIM because recognition of DMARC is still low. We feel that in the future there will be a continued need to promote the benefits of DMARC, as well as methods for its implementation.

Another distinctive point regarding the DMARC authentication ratios in Figure 4 is that the ratio of "fail" authentication results is high at 4.6%. SPF authentication is prone to fail when mail is forwarded, and there have been moves to declare an SPF record to produce less severe "softfail" results when this phenomenon is expected. For this reason, it is possible to anticipate the ratio of "softfail" results using SPF would be the high figure of 13.4%. However, compared with the 2.4% of "hardfail" results when stronger authentication fails using SPF, and the 0.7% of "fail" results for DKIM, it could be said the 4.6% of results indicating failed DMARC authentication is very high. We will analyze the reasons for this in the next section.

2.3.3 Causes of Success or Failure in DMARC Authentication

With DMARC, when either SPF or DKIM authentication succeeds, DMARC authentication is evaluated if the domain in the "From:" email header declared a DMARC record. In other words, when the DMARC authentication result is a "pass," it means that domain (RFC5322.From) and the domain authenticated using SPF or DKIM are a match or are associated, and either the SPF or DKIM authentication result was a "pass." Consequently, we tried analyzing the factors behind "pass" results for DMARC authentication. The results are shown in Figure 7.

When a DMARC "pass" result is produced, the most prevalent pattern for SPF and DKIM authentication results was cases where both methods passed, at 69.8% of the total. In short, we found that the majority of domains that declared a DMARC record and passed DMARC authentication correctly implemented both SPF and DKIM. In cases where either SPF or DKIM authentication failed or was not implemented, and DMARC authentication passed because the other method passed, SPF pass results were most

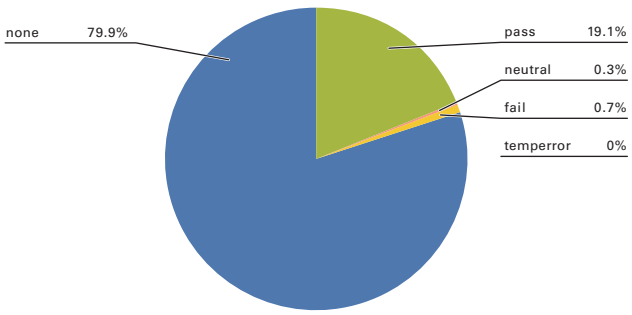


Figure 6: DKIM Authentication Result Ratios for Incoming Mail

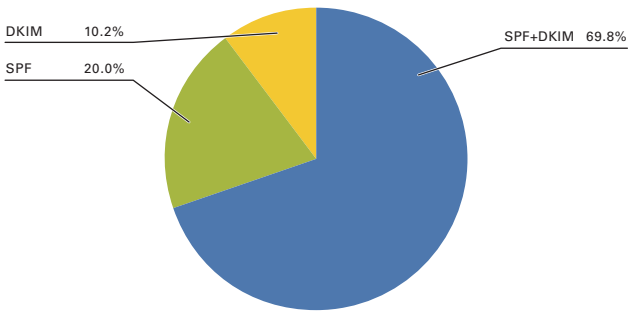


Figure 7: DMARC Pass Factors

frequent at 20.0% The ratio of cases where only DKIM authentication passed was around half that, at 10.2%. We surmise that the high deployment ratio of SPF has carried over to affect the DMARC authentication “pass” results.

Next, we will indicate the most common patterns in SPF and DKIM authentication when DMARC authentication failed in Figure 8.

The most prevalent pattern for SPF and DKIM authentication results when DMARC failed was cases in which only SPF authentication was carried out (DKIM was a “none” result), and the SPF authentication result was “fail.” Conversely, cases in which DMARC failed due to a DKIM authentication “fail” result when only a DKIM authentication result was used amounted to an extremely low ratio of just 0.6%. We believe these results demonstrate the differences in adoption rates between SPF and DKIM, as well as the robustness of DKIM authentication. Cases in which both SPF and DKIM failed made up just 0.7% of the total. Based on these factors, we found that implementing DKIM is an effective way to prevent DMARC authentication failing.

Among the DMARC failure factors, the 10.6% ratio labeled “DMARC” indicates the percentage for which DMARC authentication failed due to a mismatch between the domain authenticated using SPF or DMARC and the RFC5322.From domain authenticated using DMARC. If these were cases in which only the RFC5322.From domain is used as the misrepresented source by spoofing the sender information in SPF or DKIM, this would be a good example of correctly detecting fraudulent activity. However, if these were legitimate emails failing authentication, they could be considered unfortunate cases in which the process failed because the domains to authenticate were different, despite implementing SPF or DKIM and declaring a DMARC record. It appears that in some of these cases mail delivery has been entrusted to another provider, and the failure is caused by the SPF or DKIM authenticated domain being authenticated using the domain of the outsourcing company, resulting in a domain mismatch. Some of the mail I have received, such as email newsletters sent from major banks or other organizations, has also failed DMARC authentication for this reason. Mail sender information indicates the source of mail, so the domain used with SPF or DKIM should also be applied in a way that makes it easily and correctly identifiable as the sender’s domain.

The “none” ratio shown in Figure 8 indicates the pattern in which DMARC authentication produces a “fail” result despite the fact that the authentication result for both SPF and DKIM is “none.” This is another instance in which it would be good for DMARC if this could be detected as fraudulent activity, but it seems this is not always the case. Upon further investigation, it appears this can also be attributed to a system called Organizational Domains, in which the RFC5322.From domain that is a characteristic of DMARC and higher-level domains are treated as domains for the same organization. In other words, although the mail sent does

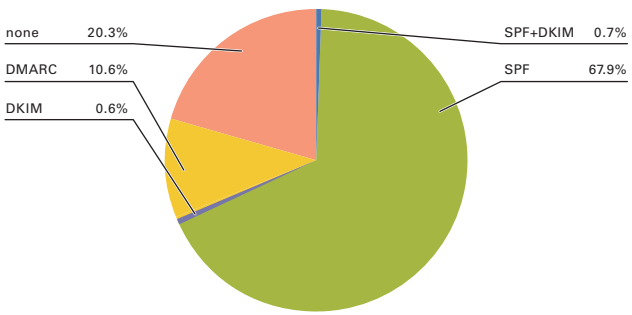


Figure 8: DMARC Failure Factors

not support either SPF or DKIM, a higher-level domain than the RFC5322.From domain in the header is declaring a DMARC record, so an attempt is made to authenticate using DMARC, producing a "fail" result. We recommend that domain administrators also configure SPF or DKIM for subdomains when declaring a DMARC record.

2.3.4 Trends in Technologies Related to DMARC

In previous IIR we have discussed that DMARC authentication can sometimes fail even for legitimate mail when resending mail, such as when sending emails to mailing lists or forwarding mail. This issue is also recognized by the organizations evaluating the specifications for DMARC, and ARC (Authenticated Received Chain)*5 has been proposed as a specification for remedying the problem. As the name suggests, this technology attempts to create an authenticated chain by linking information that is already authenticated at times such as when mail is resent. We would like to take a look at this system once the ARC specifications have been further clarified.

2.4 Conclusion

The ratio of spam began to decline gradually from 2010, but as announced in this report, there was a period in which it rose temporarily. It is said that the reason for the decrease up until now is the effectiveness of ongoing measures to prevent the activity of botnets, which are the main methods used to send spam. Hopefully this recent spike is just temporary, but we believe circumstances that enable this kind of mass-mailing capacity to continue to exist pose a threat.

Ongoing vigilance is also required with regard to the qualitative issues of spam. A high rate of incidents thought to result from spam in which monetary damage or information leaks have been caused also continue to take place in Japan. These damages are said to be related to malicious malware. There are no doubt cases in which mail is used to send this directly, or used as a trigger to infect PCs with malware. To maintain email as a fundamental communication tool, a framework for even more robust countermeasures may be necessary.

As an example of this kind of countermeasure framework, in the last IIR (Vol.27) we examined the combination of sender authentication technology centered on DMARC, domain reputations for evaluating authenticated domains, and the feedback loop for raising the accuracy of reputations. The interconnection of each of these elements improves functionality in some respects. Consequently, it would be ideal if all would become more popular, but first we hope to see DMARC become a little more widespread in Japan, as this technology can be implemented easily by senders, and has already been standardized. It is also gaining prominence in the global environment. First, we have investigated and discussed DMARC authentication result ratios in this report to better ascertain the current adoption status. We will continue to conduct a range of studies to contribute to the popularization of effective countermeasure technology.

Author:
Shuji Sakuraba
Mr. Sakuraba is a Senior Engineer in the Application Service Department of the Network Division, IIJ.
He is engaged in the research and development of communication systems. He is also involved in various activities in collaboration with external related organizations for securing a comfortable messaging environment.
He has been a member of M3AAWG since its establishment. He is acting chairperson of the Anti-Spam mail Promotion Council (ASPC) and a member of its administrative group, as well as chief examiner for the Technology Workgroup.
Additionally, he is chairman of Internet Association Japan's Anti-Spam Measures Committee.

*5 Authenticated Received Chain (ARC), draft-andersen-arc-04 (https://www.ietf.org/id/draft-andersen-arc-04.txt).

TLS Trends

There has recently been heated discussion regarding TLS (Transport Layer Security) in the IETF (Internet Engineering Task Force). The reason the debate has become so lively is without a doubt the disclosure of the U.S. government's top-secret PRISM surveillance and intelligence gathering program by Edward Snowden in 2013. With the existence of the pervasive monitoring typified by PRISM being brought to light, the IETF was forced to revisit the issue of privacy. As stated in RFC 7258, protocols drafted by the IETF in the future will be designed to make pervasive monitoring more difficult.

As far as HTTP is concerned, the use of TLS will likely be highly recommended. In fact, when using HTTP/2 protocol that was published in 2015 (RFC 7540), the use of TLS is effectively mandatory because major browsers will require it. Of course, use of TLS is also strongly recommended with the current mainstream HTTP/1.1 protocol. HTTP servers must have certificates to use TLS. Until now the issuing of certificates cost money, and that discouraged many people from using TLS. It is now also possible to issue certificates for free due to the Let's Encrypt project.

The latest version of TLS is 1.2, and eight years have passed since it was standardized. Over this period of time, a variety of attack techniques that target TLS have been discovered. RFC 7457 is an outstanding document that provides a summary of these attack techniques. As new attack methods have appeared and various cryptographic technologies have become obsolete, the recommended methods for using TLS have also changed. The currently recommended methods are detailed in RFC 7525. The IETF is now working on the draft for TLS 1.3 based on this knowledge. In this article we will give an explanation of trends in TLS targeted at those who already know its mechanisms.

3.1 Versions

The previous incarnation of TLS was the SSL (Secure Socket Layer) protocol designed by Netscape Communications. The SSL 2.0 specification was published in 1995, and SSL 3.0 was published in 1996. There were a variety of issues with the design of SSL 2.0, and use of it was prohibited by RFC 6176. SSL 3.0 also had issues with attacks such as the POODLE vulnerability, as well as flaws in its design, and RFC 7568 required that it not be used.

SSL was brought in to the IETF and standardized, at which point it became TLS. TLS versions 1.0, 1.1, and 1.2 have been established. I will go into more detail later, but currently the use of a method called AEAD (Authenticated Encryption with Associated Data) is recommended for data authentication and encryption. AEAD cannot be used with TLS 1.0 or 1.1. Getting straight to the point, to use TLS safely it is now necessary to utilize TLS 1.2 via a suitable method.

Table 1 shows a summary of information regarding SSL/TLS versions (ID is an abbreviation of Internet-Draft). We will also discuss TLS 1.3 in this article, but as its specifications are currently being drawn up, please understand that it may end up slightly different.

Version	Specification	Year Established	Usage
SSL 2.0	Stopped at ID	1995	Use prohibited by RFC 6176
SSL 3.0	RFC 6101	1996 (RFC issued in 2011)	Use prohibited by RFC 7568
TLS 1.0	RFC 2246	1999	△
TLS 1.1	RFC 4346	2006	△
TLS 1.2	RFC 5246	2008	○
TLS 1.3	ID	Draft underway	

Table 1: SSL/TLS Versions

3.2 Suitable Cipher Suites

RFC 5246 in which TLS 1.2 was established requires that the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite be implemented. This has the following meaning:

- RSA for key exchange
- RSA also for server authentication
- AES in CBC mode for the encryption of communications
- SHA1 for the MAC generation function

The TLS 1.2 cipher suite required by HTTP/2 and recommended for first proposal in RFC 7525 is TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256. This is interpreted as follows:

- ECDHE (Elliptic Curve Diffie-Hellman, Ephemeral) for key exchange
- RSA for server authentication
- AES 128 in GCM (Galois/Counter Model) mode for the encryption of communications
- SHA256 for the secure hash function

In TLS 1.3, the implementation of TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 is required in addition to TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256. Server authentication has merely changed from RSA to ECDSA (DSA using elliptic curve cryptography).

Next, I will explain the reasons why the recommended cipher suites have changed in this way.

3.3 Public-Key Cryptography and Key Exchange

As mentioned above, the recommended key exchange method has changed from RSA to ephemeral Diffie-Hellman keys. This is because ephemeral Diffie-Hellman keys provide forward secrecy, which RSA lacks. Forward secrecy means that the secrecy of data is protected going forward.

Let us look at why there is no forward secrecy when RSA is used for key exchange. When a client connects to a server using TLS, the server sends a certificate to the client. This certificate consists of the server's public key signed by a certificate authority. The client generates the secret it needs to share with the server, and encrypts it with the server's RSA public key before sending it to the server. Only a server with the RSA private key can decrypt this ciphertext. This means the client and server have successfully shared secret data, so symmetric-key cryptography is used to protect the communication channel using a key generated from this secret.

At this point, the encrypted channel is secure. It is almost impossible for a third party to intercept content. However, if the following events were to actually occur, communications could be intercepted.

Let us suppose that certain pervasive monitoring has captured all the data carried over this encrypted channel. Then, when the server is destroyed due to it being swapped out, the data on the hard disk was not erased by mistake. If the party performing pervasive monitoring were to obtain this hard disk, it could extract the private key, so it would be possible to decrypt the saved encrypted channel data in sequence.

Meanwhile, with ephemeral Diffie-Hellman methods, the client and server both generate temporary public and private keys. These private keys are not saved to the hard disk, so the aforementioned example would not happen.

It seems that the ECDHE (RFC 4492) ephemeral Diffie-Hellman method achieved through elliptic curve cryptography is more likely to see widespread use than the original DHE (Diffie-Hellman, Ephemeral). This is because of the following:

- ECDHE exchanges less data than DHE.
- The computation rate of ECDHE is faster than DHE.
- ECDHE has carefully-selected parameters defined in advance. Although there is an ID aimed at defining parameters for DHE, it has not yet reached the RFC stage.
- As mentioned earlier, ECDHE is listed as the suite for first proposal in RFC 7525.

See "1.4.2 Forward Secrecy" in IIR Vol.22 for more information about forward secrecy.

3.4 The Obsolescence of Symmetric-Key Cryptography

TLS 1.1 and earlier uses the following two ciphertext formats.

- Stream ciphers
- CBC (Cipher Block Chaining) mode block ciphers

A range of attack methods have been found in RC4, which is the only practical option for stream ciphers, so their use is prohibited (RFC 7465).

With regard to TLS 1.0 and earlier CBC mode block ciphers, the BEAST attack method is well known. Additionally, the "MAC-then-encrypt" method is used with TLS 1.2 and earlier CBC mode block ciphers. A MAC (Message Authentication Code) is auxiliary data for ensuring data has not been altered and authenticating it. MAC-then-encrypt involves generating a MAC from plaintext, then appending this MAC to the plaintext and encrypting the result. An attack technique called padding oracle attacks that targets MAC-then-encrypt has been found. For this reason, the "encrypt-then-MAC" format is proposed in RFC 7366 as a replacement for MAC-then-encrypt.

In TLS 1.2, AEAD (Authenticated Encryption with Associated Data) was specified as a third format for ciphertext. AEAD is a method in which encryption and authentication are carried out simultaneously. Currently, the use of AEAD is recommended instead of stream ciphers or CBC mode block ciphers. The following symmetric-key encryption modes can be used with AEAD:

- AES-GCM (Galois/Counter Model) mode
- AES-CCM (Counter with CBC-MAC) mode

In TLS 1.3, the stream cipher and CBC mode block cipher formats have been deleted, so only AEAD is defined.

3.5 Handshake

In this section, I will explain actual TLS communications.

3.5.1 Full Handshake

When a client first connects to a server, a full handshake must be performed. In TLS 1.2, the process shown in Figure 1 takes place when TLS_RSA_WITH_AES_128_CBC_SHA is selected.

- The client advertises the cipher suites it supports in a ClientHello message.
- The server indicates it has selected TLS_RSA_WITH_AES_128_CBC_SHA in a ServerHello message. The server's RSA certificate is included in the Certificate message.
- The client generates a secret, encrypts it with the server's RSA public key, and sends it stored in a ClientKeyExchange message. A ChangeCipherSpec message is then sent to switch the communication channel to an encrypted channel. This channel is encrypted using AES-CBC mode. Immediately after switching to an encrypted channel, a Finished message is sent to confirm that the handshake concluded successfully. All data subsequently received from applications is also sent using this encrypted channel. The gray parts of Figure 1 indicate the encrypted channel.

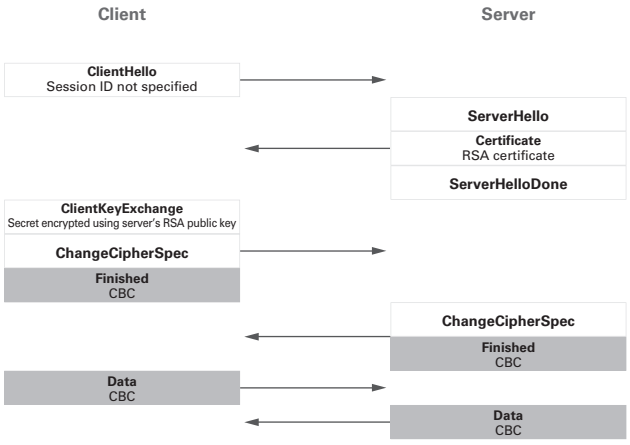


Figure 1: TLS 1.2 Full Handshake TLS_RSA_WITH_AES_128_CBC_SHA

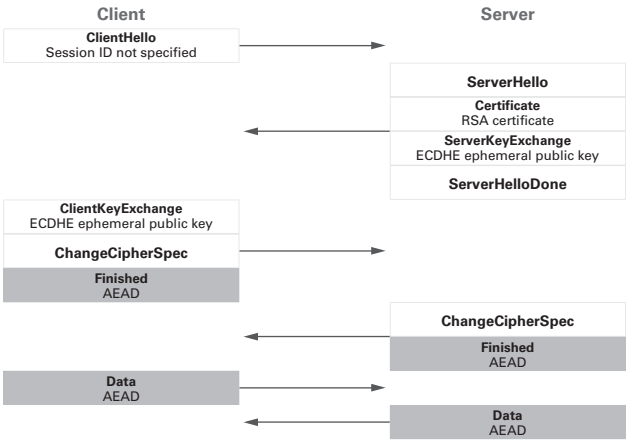


Figure 2: TLS 1.2 Full Handshake TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

- The server uses its private key to extract the secret, and in the same way as the client sends a ChangeCipherSpec message to switch the communication channel to an encrypted channel.

Next, I will discuss what happens when TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 is selected in TLS 1.2 (Figure 2). The differences compared to TLS_RSA_WITH_AES_128_CBC_SHA are as follows:

- After the server receives the ClientHello, it selects TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256. Then, it generates ECDHE ephemeral public and private keys. The public key is sent inside a ServerKeyExchange message.
- The client also generates ECDHE ephemeral public and private keys. It generates a secret from its private key and the server's public key. Its public key is sent inside a ClientKeyExchange message.
- The server generates a secret from its private key and the client's public key.

The full handshake process doesn't change at all for TLS 1.0, 1.1, or 1.2. However, the full handshake process has been radically redesigned in TLS 1.3. Above all, it reduces the RTT (Round Trip Time) by one step by handling key exchange in the Hello message.

- The client creates ECDHE ephemeral public and private keys, and sends the public key stored in a ClientHello message option.
- The server also creates ECDHE ephemeral public and private keys, and sends them stored in a ServerHello message option. The communication channel is immediately encrypted from this point. The Certificate and Finished messages that store server certificates are sent encrypted. After the Finished message is sent, a switch is made to an even more secure encrypted channel. The different shades of gray in Figure 3 indicate these different encrypted channels.
- After sending a Finished message over the current encrypted channel, the client switches to a more secure encrypted channel.

3.5.2 Resuming a Session

Once a client and server have performed a full TLS 1.2 handshake, the key exchange process can be omitted by resuming that session. Take a look at Figure 4.

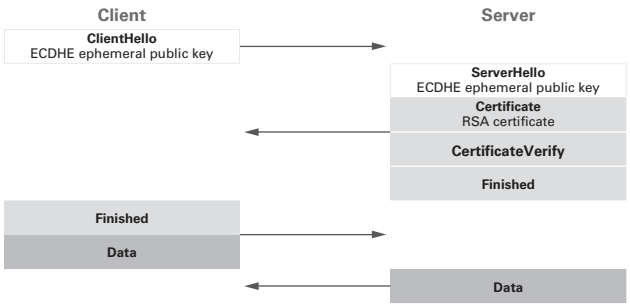


Figure 3: TLS 1.3 Full Handshake TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

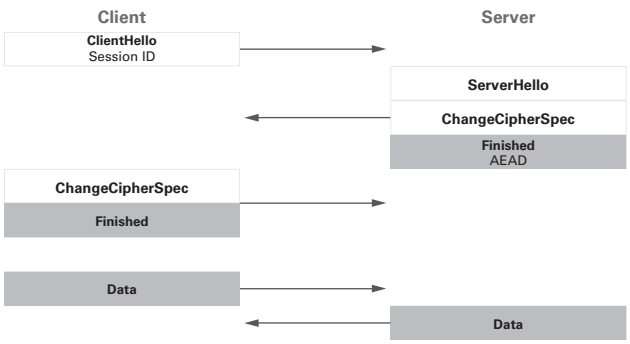


Figure 4: TLS 1.2 Session Resumption

- The client specifies the session ID for the session it would like to resume in the ClientHello message.
- If the server has saved the status of the specified session ID, it uses this to switch to an encrypted channel.

In addition to eliminating the need for heavy public key cryptography calculations, resuming a session also reduces the RTT by one step. However, this method requires that

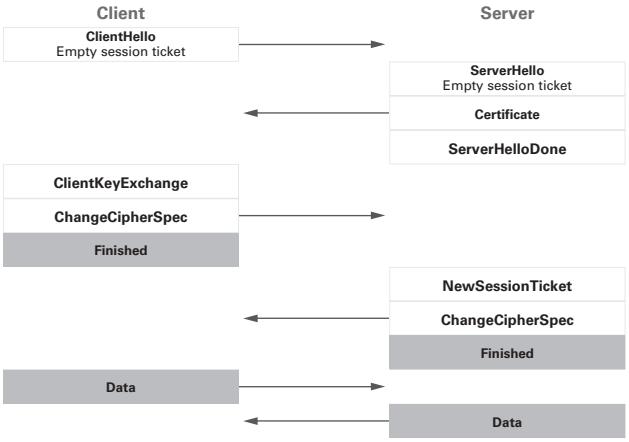


Figure 5: Full Handshake for TLS 1.2 Session Tickets

servers save session information. The amount of status data that must be retained also increases in proportion to the number of clients. This method increases the load on the server, which isn't exactly ideal.

The session ticket method defined in RFC 5077 is one way to reduce this server load. Session tickets are encrypted session information that only the server can decrypt. Using session tickets does away with the need for servers to retain session information. To use session tickets with TLS 1.2, it is first necessary to perform a full handshake for the session tickets (Figure 5).

- The client sends an empty session ticket as an extension of the ClientHello message to notify the server that it supports session tickets.
- The server also notifies the client that it supports session tickets by specifying an empty session ticket in the ServerHello options.
- Immediately before switching to an encrypted channel using ChangeCipherSpec, the server sends the session ticket it has generated in a NewSessionTicket message.
- The client associates the session ticket it was sent with the current session information, then saves it.

Next, I will explain how to resume a session using session tickets in TLS 1.2 (Figure 6).

- The client extracts the session information and session ticket to resume, and sends the session ticket in the ClientHello options.
- The server decrypts the session ticket to obtain the session information. If necessary, new session information is sent in a NewSessionTicket message. The server then switches to an encrypted channel.
- The client uses the aforementioned session information to switch to the encrypted channel.

TLS 1.3 session tickets are integrated with the PSK (Pre-Shared Key) defined in RFC 4297. The PSK method involves the use of a pre-shared secret instead of a public key for server or client authentication. If the TLS 1.3 PSK handshake is only used for the session ticket function, it doesn't differ much from TLS 1.2 (Figure 7). The minor differences are as follows:

- After a full handshake, the server can send NewSessionTicket messages at any time.
- As with the TLS 1.3 full handshake, the encrypted channel switches twice.

3.5.3 Client Authentication Using Certificates

Let us consider a case in which a certain server is accessing a certain page using TLS. We will assume the links on that page all point to the same server, but the content requires certificate-based client authentication.

In TLS 1.2, renegotiation is carried out when certificate-based client authentication becomes necessary at some point. This involves performing the handshake process again. Unlike a full handshake, this handshake is performed within the encrypted channel (Figure 8).

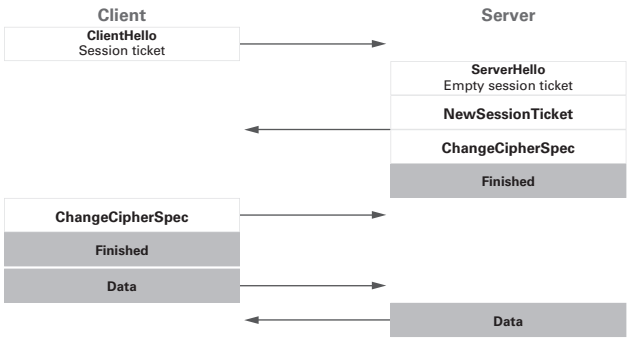


Figure 6: Resuming a Session Using TLS 1.2 Session Tickets

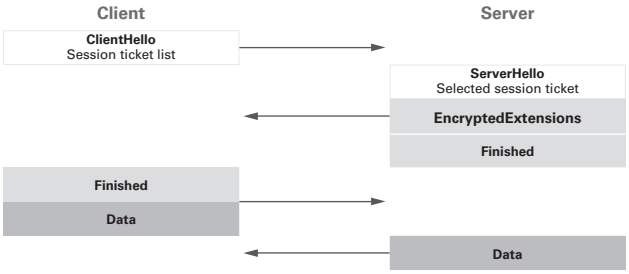


Figure 7: Resuming a Session Using TLS 1.3 Session Tickets

- The server sends a HelloRequest message to the client requesting renegotiation.
- The client sends a ClientHello message.
- The server sends a CertificateRequest along with the ServerHello message requesting the client's certificate.
- The client sends the client certificate in a Certificate message when sending the ClientKeyExchange message.

The original purpose of renegotiation is to refresh and extend the life of the encrypted channel. It is also used for certificate-based client authentication due to the limitation in TLS 1.2 that requires CertificateRequest messages to be sent immediately after the ServerHello message.

In TLS 1.3, a clear distinction is made between refreshing the encrypted channel and certificate-based client authentication. This enables CertificateRequest messages to be sent from the server to the client at any time (Figure 9).

3.5.4 0-RTT

In TLS 1.3, a handshake mode called 0-RTT that also encrypts and sends application data when sending a ClientHello message is under consideration. This is a little complicated, so I'll skip the explanation for now. Anyone interested should refer to the TLS 1.3 ID.

3.6 Compression

In TLS 1.2 and earlier, there is a compressed text format in addition to plaintext and ciphertext. When using a compression function, plaintext is compressed into compressed text, then this is encrypted to create ciphertext. Unfortunately, when a compression function is used, the text is vulnerable to attacks such as CRIME and BREACH.
For this reason, you cannot use compression functions when using TLS 1.2. Encrypt plaintext directly to create the ciphertext. In TLS 1.3, the compressed text format has been deleted, and only plaintext and ciphertext are defined.

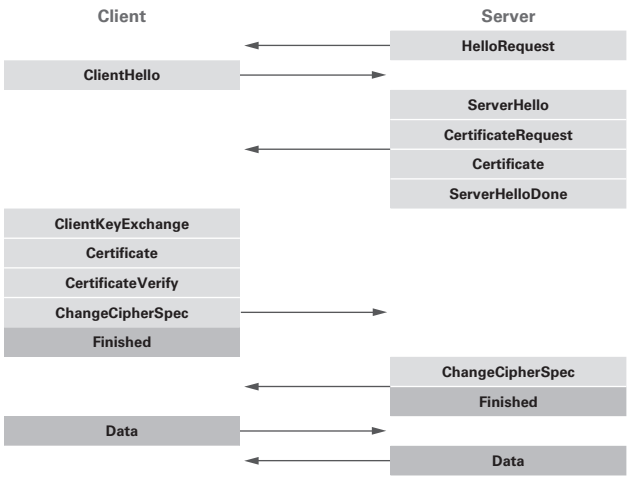


Figure 8: Certificate-Based Client Authentication Using TLS 1.2

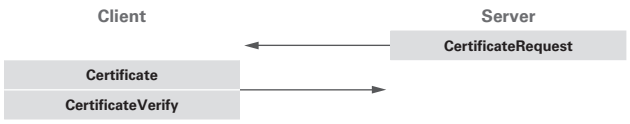


Figure 9: Certificate-Based Client Authentication Using TLS 1.3

3.7 Let's Encrypt

Let's Encrypt is a project for automatically issuing free server certificates. Only Domain Validation (DV) certificates can be issued, so the issuing of Organization Validation (OV) or Extended Validation (EV) certificates is not possible. At this point in time, wildcard certificates cannot be issued. When there are multiple server names, you can either request the issue of enough DV certificates to match the number of servers, or you can use a Subject Alternative Name (SAN). The commands provided by Let's Encrypt implement the ACME (Automatic Certificate Management Environment) protocol that the IETF is currently working on standardizing. See "1.4.2 The Let's Encrypt Project and the ACME Protocol for Automatic Certificate Issuing" in IIR Vol.30 for more information about Let's Encrypt.

3.8 Final Remark

In this article, I have only given the names of attack techniques, and not explained the specific methods involved. More detailed explanations of each attack technique can be found easily by searching online. Anyone interested should look up this information to find out more.

Author:
Kazuhiko Yamamoto
Senior Researcher, Research Laboratory, IIJ Innovation Institute Inc.
Mr. Yamamoto is interested in applying the parallel technology of the Haskell programming language to network programming.
Recently he has been working on the HTTP/2 and TLS 1.3 protocols.
He has translated the books "Programming in Haskell" and "Parallel and Concurrent Programming in Haskell".

June 2016 Vol.31

IIJ
Internet Initiative Japan

About Internet Initiative Japan Inc. (IIJ)

IIJ was established in 1992, mainly by a group of engineers who had been involved in research and development activities related to the Internet, under the concept of promoting the widespread use of the Internet in Japan.

IIJ currently operates one of the largest Internet backbones in Japan, manages Internet infrastructures, and provides comprehensive high-quality system environments (including Internet access, systems integration, and outsourcing services, etc.) to high-end business users including the government and other public offices and financial institutions.

In addition, IIJ actively shares knowledge accumulated through service development and Internet backbone operation, and is making efforts to expand the Internet used as a social infrastructure.

IIJ-MKTG020-0029

Internet Initiative Japan Inc.

Address: Iidabashi Grand Bloom, 2-10-2 Fujimi, Chiyoda-ku,
Tokyo 102-0071, Japan
Email: info@iij.ad.jp URL: http://www.iij.ad.jp/en/