LAC
株式会社ラック

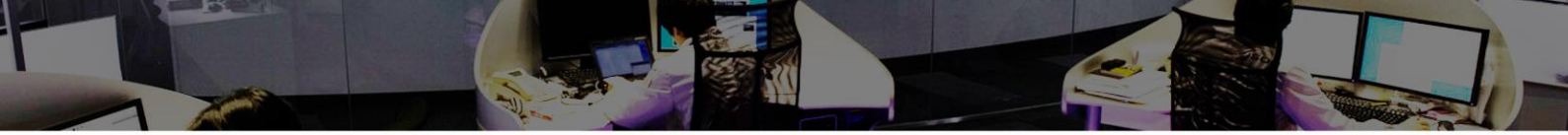
INSIGHT

vol.9

January 27, 2016

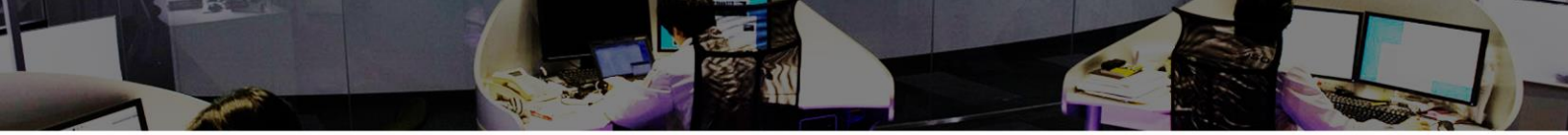
JSOC Analysis Team

JSOC JAPAN SECURITY OPERATION CENTER



JSOC INSIGHT vol.9

JAPAN SECURITY OPERATION CENTER



1 Preface

The Japan Security Operation Center (JSOC) is a security monitoring center operated by LAC Co., Ltd. that provides security monitoring services, such as "JSOC Managed Security Services (MSS)" and the "24+ Series." The JSOC MSS maximizes the performance of security devices through unique signatures and tuning, and our security analysts, with their expert knowledge, analyze logs from security devices in real time, 24 hours a day, 365 days a year. In this real-time analysis, the security analysts pour over communication packets in detail, down to their content level, as well as diagnose whether monitored objects are affected and whether there are any vulnerabilities and other potential risks, for every occasion, all in order to minimize misreporting from security devices. We help our customers to improve their security level by reporting only critical incidents needing an emergency response in real time and by taking action against attacks in the shortest time possible.

This is an analysis report on the trend of security incidents, such as unauthorized access and malware infection, in Japan, based on the daily analysis results of our JSOC security analysts. As this report analyzes the trend of attacks, based on the data of incidents that JSOC customers have actually encountered, the report will aid the understanding of world trends, as well as the actual threats that Japanese users are currently facing.

We really hope that this report will provide our customers with useful information that can be made full use of when implementing countermeasures to improve security.

Japan Security Operation Center

Analysis Team

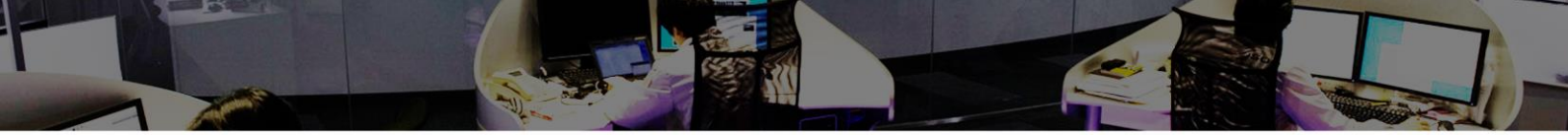
Data collection period

April 1, 2015 to June 30, 2015

Devices used

This report is based on data from security devices supported by the LAC-supplied JSOC Managed Security Services.

* This document is for information purposes only. LAC Co., Ltd. takes no responsibility for any loss resulting from using this document.
* When using data from this report, be sure to cite the source. (For example, “Source: JSOC INSIGHT, vol. 9, from LAC Co., Ltd.”)
* The information contained in this document is as of the initial publication of this document and may be changed by the time it is viewed or provided.



2 Executive Summary

This report analyzes the trends in the incidents that occurred from April to June, 2015, and introduces especially notable threats.

➢ Malware infection due to targeted attacks

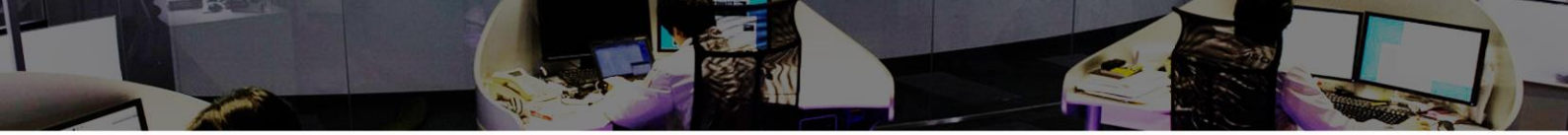
The JSOC has detected traffic infected with a certain type of malware known as "Emdivi," which is considered to have been used to let information leak from the Japan Pension Service. The Emdivi infection is characterized by having no bias in the industry or business type of the customers for which infected traffic was detected, and infection was detected for a variety of companies. It is also characterized such that many of the malware codes detected so far have communicated with overseas C2 servers, but also that many of the terminals infected with Emdivi communicated with C2 servers from a Japanese domain. Also, as there have been almost no Emdivi infections detected overseas, Japan is considered to be the target of attack.

➢ Attack traffic that exploits a vulnerability in HTTP.sys file processing

It was disclosed that a Web server (IIS) implemented in specific versions of Windows had a vulnerability that allows for a denial of service and the execution of any command. A method that exploits the vulnerabilities very easily to restart its target has been disclosed, and the JSOC detected attacks using such method. No attack code that allows for command execution has been confirmed.

➢ Denial-of-service vulnerability in PHP

A vulnerability in specific versions of PHP that causes a denial of service externally was disclosed. The method that exploits the vulnerability is very easy to implement. The JSOC has not detected any attack traffic that exploits the vulnerability, but it is necessary to take quicker actions, as such an attack will have a significant negative impact.



3 Trends in Severe Incidents at the JSOC

3.1 Trends in severe incidents

Our security analysts at the JSOC pour over the logs detected by IDS/IPS, sandboxes, and firewalls, and assign one of four incident severity levels according to the nature of incident and the degree of impact that the incident has on monitored targets. Of the four severity levels, Emergency and Critical indicate severe incidents for which the likelihood of a successful attack occurring or causing serious damage is high.

Table 1 Incident severity levels

Type	Severity	Description
Severe incident	Emergency	Incident for which a successful attack is confirmed
	Critical	Incident for which the likelihood of a successful attack is high or for which a failed attempt at an attack is not confirmed This indicates that the incident is due to malware infection.
Reference incident	Warning	Incident for which a failed attempt at an attack is confirmed or no real damage is confirmed
	Informational	Incident that does not trigger an attack causing any real damage and has no significant impact, such as scanning

Figure 1 shows the changes in the number of severe incidents from April to June 2015.

The number of severe intra-network incidents was on the decrease from April to June, and the number of such incidents of June is half that of April. The decrease is due to the fact that some customers who had detected malware infection since March completed incident handling around the end of May. During the fifth week of April and the first week of June, the JSOC detected traffic deemed to be infected with malware through targeted attacks ([1] and [2] in Figure 1).

The number of severe incidents related to attacks from the Internet increased between the second week and fourth week of May 2015 ([3] in Figure 1). This is because the number of severe incidents increased due to attacks that had been detected so far, including suspicious file upload attempts and SQL injections.

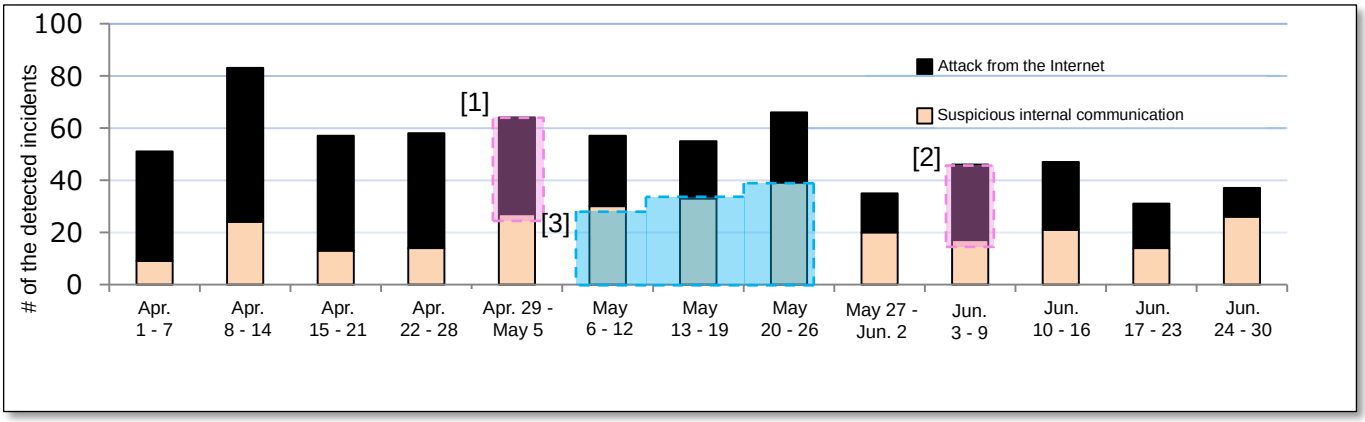
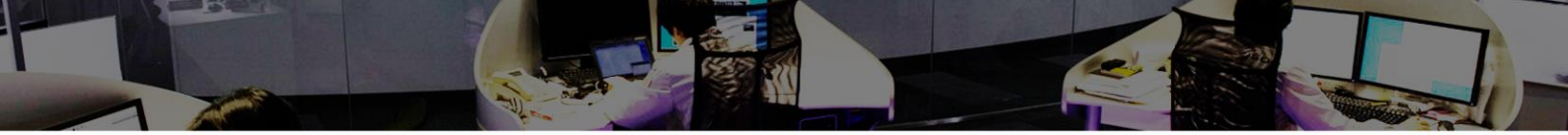


Figure 1 Changes in the number of severe incidents (April to June 2015)

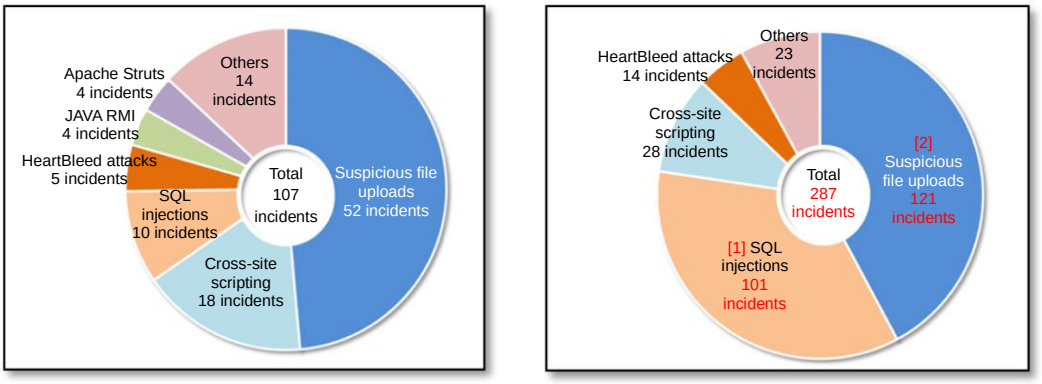


3.2 Analysis of severe incidents

Figure 2 shows a breakdown of severe incidents related to attacks from the Internet.

In the number of severe incidents related to attacks from the Internet, the period from April to June 2015 saw a significant increase (up to 287 from 107) compared to the period from January to March.

This is because similar attacks were repeated against customers who had hosts vulnerable to SQL injection (b-[1] in Figure 2). The period from April to June saw a surge in the number of severe incidents due to suspicious file upload attempts that exploited a plug-in vulnerability in WordPress and had no specific targets (b-[2] in Fig.2).



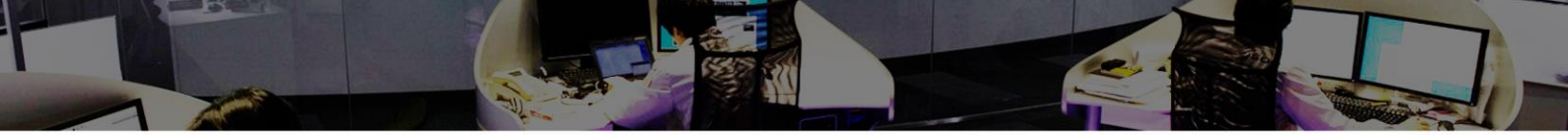
a. January to March 2015 **b. April to June 2015**

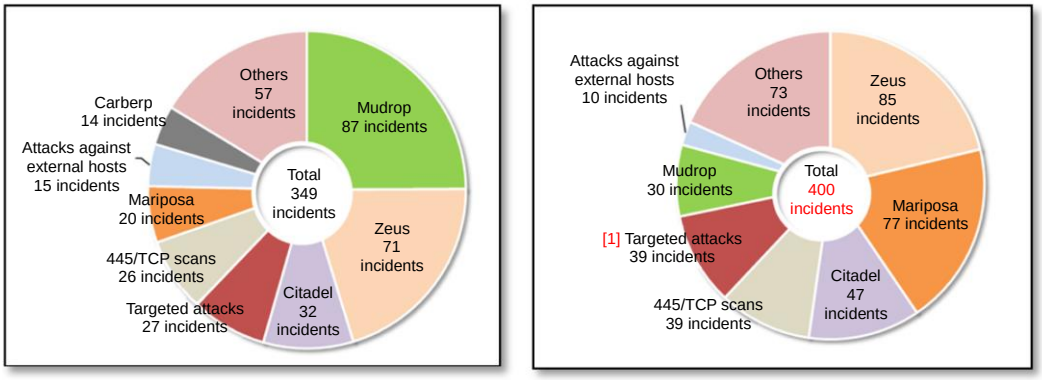
Figure 2 Breakdown of severe incidents related to attacks from the Internet

Figure 3 shows a breakdown of severe intra-network incidents.

In the number of severe intra-network incidents, the period from April to June 2015 saw a slight increase (up to 400 from 349) compared to the period from January to March. This is because, in addition to continued malware infection in some customers, there were many detections of traffic deemed to be infected with malware that targeted Internet banking information, such as Zeus/Zbot.

Further, as a result of enhanced targeted attack monitoring, based on analysis results from the Cyber Emergency Center, traffic that might be infected with malware due to a targeted attack was detected in multiple customers between April and June 2015 ([1] in Figure 3 b).





a. January to March 2015 **b. April to June 2015**

Figure 3 Breakdown of severe intra-network incidents

3.3 Attack traffic from the Internet that has been detected many times

Table 2 shows the attack traffic from the Internet that has been detected especially many times between April and June 2015. In many of the cases, the target is discriminately attacked, regardless of whether a specific Web application was used in it, and the attempt failed. However, depending on the condition of the target, resources might be consumed excessively due to heavily increased attack traffic.

For this period, many occurrences of these traffic attacks in this period lead to a large amount of analysis cost, and JSOC analysts in charge of real-time monitoring have often suffered.

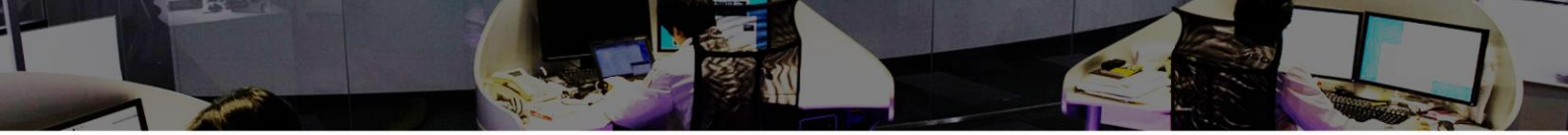
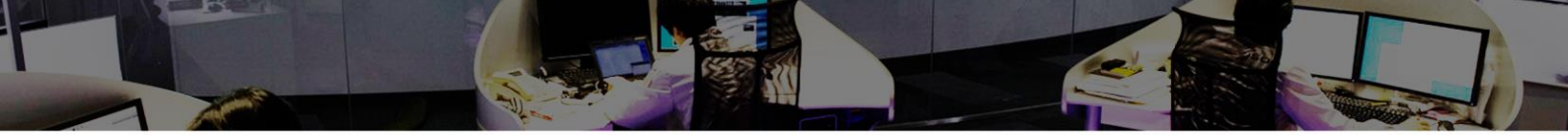


Table 2 Attack traffic from the Internet that has been detected many times

Attack type	JSOC detection	Detection period	Severe incidents
Shellshock	Traffic for checking for the existence of Shellshock[1] vulnerability and attacks that attempt to exploit hosts have been detected continually. Diversified commands are used in these attacks.	To the beginning of May 2015	No
Attacks against phpMoAdmin	Attempts to execute a command against phpMoAdmin[2] have been detected. The command used in the attacks attempts to display the host information of the target.	Beginning of June 2015	No
Attacks against OpenView NNM	Attempts that exploit a vulnerability[3] in the "OpenView NNM" HP product to execute a command have been detected. It seemed that these attacks, originating from a single host, were made against all available IPv4 addresses.	Middle of June 2015	Yes
WordPress vulnerability scan	Attempts to exploit a plug-in vulnerability in WordPress and view the configuration file or upload a suspicious file have been detected.	Attacks have not been detected during a specific time period, but occur steadily.	Yes

[1] JSOC INSIGHT vol. 7
4.1 Changes in the trends of Shellshock incidents
http://www.lac.co.jp/security/report/pdf/20150519_jsoc_m001t.pdf
[2] JSOC INSIGHT vol. 8
3.2 Code execution vulnerability in phpMoAdmin
http://www.lac.co.jp/security/report/pdf/20150713_jsoc_j001m.pdf
[3] HP support document - HP Support Center (document ID: c02215897)
http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c02215897



4 Topics of This Volume

4.1 Malware infection as a targeted attack

The JSOC works with our emergency response team, the Cyber Emergency Center, to exchange information about new attack methods and incidents. The JSOC creates JOSC original signatures (JSIG) for an attack that can be handled, based on targeted attack and malware infection information from the Cyber Emergency Center. This helps to expand the detectable range of attacks by covering suspicious traffic that cannot be dealt with via IDS or IPS vendor-supplied signatures, as well as targeted attacks focusing on particular Japanese government agencies and corporations.

Between April and July 2015, the JSOC detected traffic infected with malware due to a targeted attack in multiple monitored customers and sent an emergency notification to these customers. These incidents include traffic infected with the Emdivi malware, which is considered to have been used to let information leak from the Japan Pension Service[4].

4.1.1 Emdivi-infected traffic incidents

Figure 4 shows the changes in the number of severe Emdivi-related incidents.

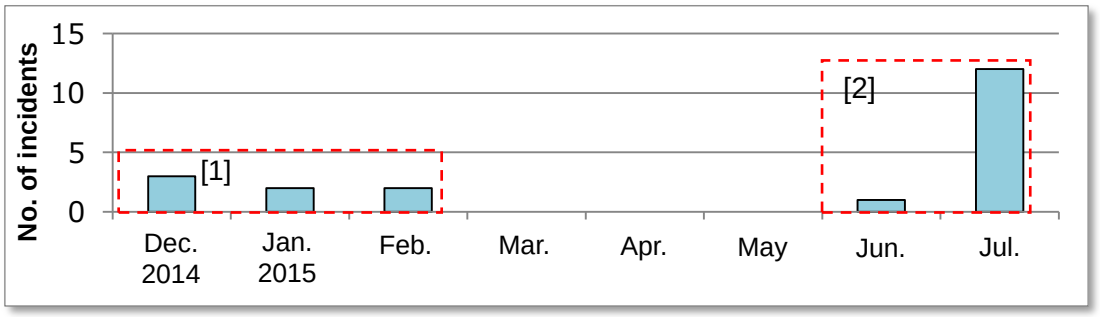
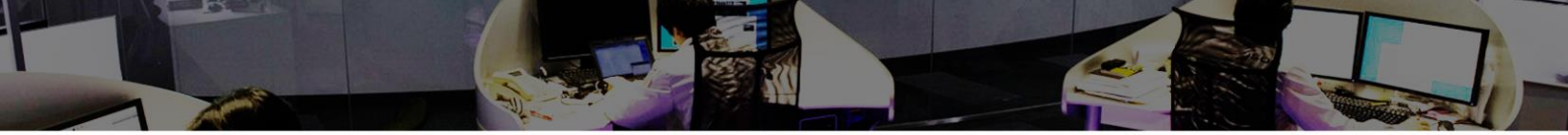


Figure 4 Changes in the number of severe Emdivi-related incidents

The JSOC detected Emdivi-infected traffic as a type of targeted attack between December 2014 and February 2015 ([1] in Figure 4). Such traffic was not detected until the end of June, but since then, traffic suspected to be infected with Emdivi has been detected in multiple customers ([2] in Figure 4).

Infection with Emdivi occurs through a drive-by download attack that triggers the download of a malicious file when a file attached to a targeted e-mail message is opened or when an altered website is viewed. Then, when the Emdivi-infected terminal is connected to an external C2 server, the attacker can operate the infected terminal remotely.

[4] Information leakage incident due to cracking at the Japan Pension Service
http://www.mhlw.go.jp/kinkyu/150603.html



In November 2014, JustSystems disclosed a vulnerability that allows any code to be executed in its Ichitaro series,[5] and the likely cause of traffic infection of that time was an executable file attached to a targeted e-mail message that exploited the vulnerability. Ichitaro is mostly used in Japan, and these attacks are considered to have targeted Japan ([1] in Figure 4).

The JSOC did not detect Emdivi from March until the middle of June, but when 2015 started, the Cyber Emergency Center noticed an abrupt increase in the number of customer requests and confirmed Emdivi infection incidents.[6] These trends may indicate that the infection phase has ended and that the phase of information acquisition from infected terminals has started.

On June 1, the Japan Pension Service announced that personal data from approx. 1.25 million pensioners and other participants in the national pension scheme, including their pension account numbers, was leaked. This is the largest incident in the history of information leakage from a public organization, attracting a great deal of attention about the targeted attack, and various institutions and corporations released reports about the incident.[7] On August 20, the Japan Pension Service and the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) released their investigation result reports about the incident,[8, 9] and then, on the next day, August 21, the Ministry of Health, Labour and Welfare released a verification report about the incident.[10]

Since the end of June, the JSOC has detected more and more Emdivi-infected traffic ([2] in Figure 4). Among customers for which such infected traffic was detected, there is no noticeable trend in the industry or business type, and it is considered that a variety of customers were discriminately attacked.

Figure 5 shows Emdivi-infected traffic examples.

An Emdivi-infected terminal triggers traffic with Get and Post requests. GET request-based traffic contains infected terminal information in its Cookie header. POST request-based traffic includes traffic that contains infected terminal information in its data portion for "index.php" or the URI of "/random number?p=#" such as "/15932?p=#".

---

[5] Suspicious program that exploits a vulnerability in Ichitaro and its risk
http://www.justsystems.com/jp/info/js14003.html

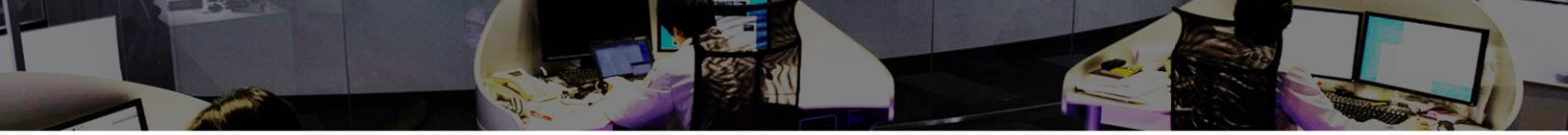
[6] Attention! Cyber espionage surging behind the scenes
http://www.lac.co.jp/security/alert/2015/06/16_alert_01.html

[7] Release Notice - "Lessons that we can learn from the information leakage incident at the Japan Pension Service"
http://www.lac.co.jp/news/2015/06/09_news_01.html

[8] Investigation results about information leakage incidents due to cracking
https://www.nenkin.go.jp/oshirase/press/2015/201508/20150820-02.files/press0820.pdf

[9] Investigation results to determine the cause of personal data leakage at the Japan Pension Service
http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf

[10] Verification report from the Committee for the Verification of Information Leakage due to cracking at the Japan Pension Service
http://www.mhlw.go.jp/kinkyu/dl/houdouhappyou_150821-02.pdf



```
GET [redacted]/index.php HTTP/1.1
Cookie: [random string]=▲▲▲&date= ■ ■ ■
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0;
Windows NT 5.1; SV1; .NET CLR 2.0.50727.42)
Host: www[redacted].com
Proxy-Connection: Keep-Alive

▲ : Obfuscated string of infected terminal's hostname or active process ID
■ : Obfuscated string indicating some information
```

(a) GET request-based traffic

```
POST[redacted]/index.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows
NT 5.1; SV1; .NET CLR 2.0.50727.42)
Host: www.[redacted].jp
Content-Length: 204
Pragma: no-cache
Via: 1.1 itckcc82:8080 (IWSS)
Connection: Keep-Alive

[random string]=▲▲▲&date= ■ ■ ■

▲ : Obfuscated string of infected terminal's hostname or active process ID
■ : Obfuscated string indicating some information
```

(b) POST request-based traffic (to index.php)

```
POST [redacted]/15932?p=# HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows
NT 5.1; SV1; .NET CLR 2.0.50727.42)
Host: www[redacted].com
Content-Length: 228
Proxy-Connection: Keep-Alive
Pragma: no-cache

[random string]=▲▲▲&date= ■ ■ ■

▲ : Obfuscated string of infected terminal's hostname or active process ID
■ : Obfuscated string indicating some information
```

(c) POST request-based traffic (to /random number?p=#)

Figure 5 Sample traffic from an Emdivi-infected terminal

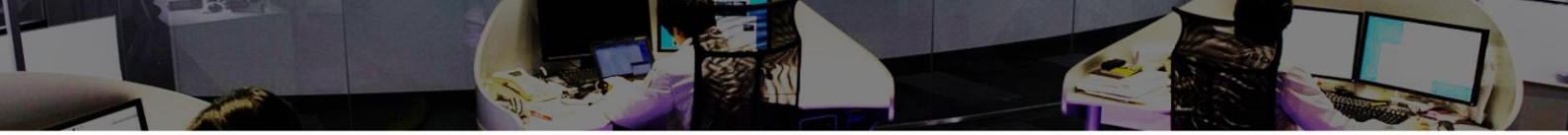


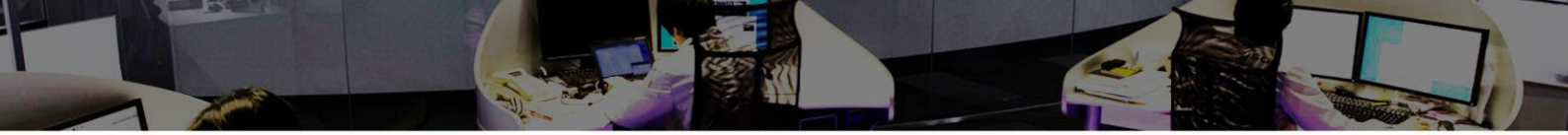
Table 3 shows the destinations of communications that originated from Emdivi-infected terminals confirmed by the JSOC.

According to the JSOC investigation, most of the communications that originated from hosts infected with malware (as a result of a targeted attack, for example) were made to C2 servers hosted overseas. On the other hand, however, most communications that originated from Emdivi-infected hosts have the characteristic such that they were made to C2 servers hosted in a Japanese domain, as shown in Table 3. Most of these destination C2 servers are websites managed by companies providing a specific cloud service. These websites are running regular Web contents, mainly including blogs, but they do not use a specific Web application. This indicates that it is unlikely that the attacker targeted a vulnerability in a specific Web application to exploit a host. The attack method is not yet clear. A possible reason why hosts used in Japan were exploited by Emdivi is to prevent a network device or the like from shutting off communication from an infected host to a C2 server.

From these conditions, it is considered that targeted attacks using Emdivi specifically target Japan and users in Japan.

Table 3 Destinations of communications that originated from Emdivi-infected terminals confirmed by the JSOC

Destination IP address	Destination domain name	Country
125.XXX.XXX.72	www. .co.jp www. .com www. .co.jp	Japan
125.XXX.XXX.79	www. .com www. .co.jp	
125.XXX.XXX.113	www. .com www. . .org	
125.XXX.XXX.114	www. .com	
203.XXX.XXX.233	www. .jp	
54.XXX.XXX.0	www. .co.jp	U.S.
–	www. .co.jp	
103.XXX.XXX.59	–	Hong Kong
203.XXX.XXX.210	www. .com	
–	www. .com	Unknown



4.1.2 Countermeasures against targeted attacks such as Emdivi

As targeted attack methods have become more sophisticated, in addition to measures that individual users take, it is necessary to implement multiple organization-level measures such as targeted attack training and the establishment of a structure for responding to possible incidents.[11, 12]

■ **Organization-level measures**

- Periodic employee training
- Collection of up-to-date threat information and others
- Establishment of an organizational incident response structure
- Incident drill for verifying response guidelines

■ **Individual user-level measures**

- Keeping the definition file of anti-virus software up-to-date
- Keeping the operating system and application software up-to-date
- Not opening any suspicious e-mail or attached file
- Installing EMET, which is available from Microsoft Corporation (for damage reduction)

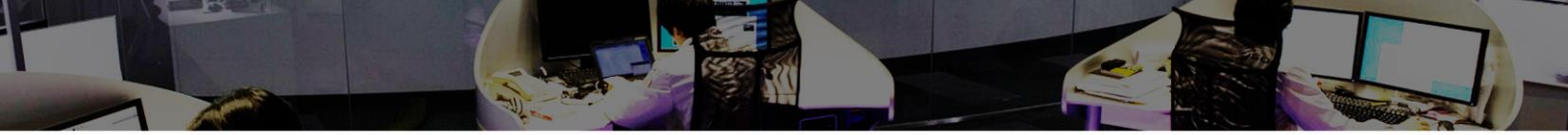
■ **Operator-level measures**

- Installing anti-virus software
- Using security devices such as firewall, next-generation firewall, IDS, IPS, or MPS for protection
- Removing any e-mail containing an executable file attachment on a system level
- Using SPF (Sender Policy Framework) to verify sender domains

In the case of an incident, it is important to collect outbound traffic logs from security devices, proxy servers, and e-mail servers, etc., for future investigation.

[11] Lessons that we can learn from the information leakage incident at the Japan Pension Service
http://www.lac.co.jp/security/report/pdf/20150609_apt_j001t.pdf

[12] Minimum countermeasures to be taken in response to the reported Japan Pension Service incident
http://www.lac.co.jp/security/report/pdf/20150831_apt_a001m.pdf



4.2 Attack traffic that exploits a vulnerability in HTTP.sys file processing

4.2.1 HTTP.sys vulnerability

It was disclosed that some functions (HTTP.sys) of IIS, a Web server implemented in specific versions of Windows, had a vulnerability (CVE-2015-1635, MS15-034) that allows for the remote execution of any command. This vulnerability causes a denial of service condition or memory leak from the content cache when handling an HTTP request containing a malicious Range header.[13, 14]

Table 4 shows the software versions that may be affected by this vulnerability when MS15-034 has not been applied and when IIS is enabled.

Table 4 Software versions that may be affected by the HTTP.sys vulnerability

Software	Version	Edition
Microsoft Windows	7	32-bit Systems SP1
		x64-based Systems SP1
	8	32-bit Systems
		x64-based Systems
	8.1	32-bit Systems
		x64-based Systems
Microsoft Windows Server	2008 R2	Itanium-Based Systems SP1
		x64-based Systems SP1 (Server Core installed)
	2012	Server Core installed
	2012 R2	Server Core installed

4.2.2 JSOC-detected attacks that target the HTTP.sys vulnerability

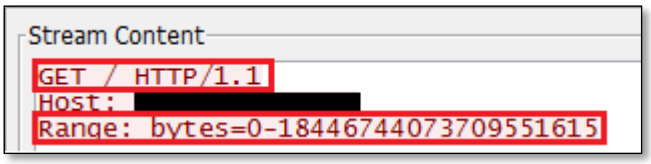
Figure 6 shows the JSOC-detected traffic that exploited the vulnerability.

The JSOC has detected different types of traffic: traffic for checking the target for the existence of a vulnerability (Figure 6a) and attack traffic that attempts to exploit the vulnerability to restart the target (Figure 6b). These types of traffic show a difference in the range start values specified in the HTTP request and Range header, and different values have different effects of attack.

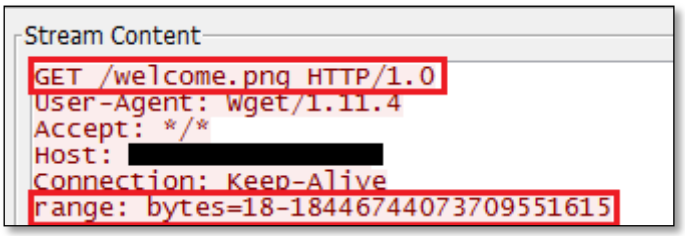
---

[13] Security TechCenter, Microsoft Security Bulletin MS15-034 – Critical
https://technet.microsoft.com/ja-jp/library/security/ms15-034.aspx

[14] A vulnerability that allows any code execution detected in HTTP.sys for multiple Microsoft Windows products
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-002263.html



(a) Traffic for checking the target for the existence of the HTTP.sys vulnerability



(b) Attack traffic that attempts to exploit the HTTP.sys vulnerability to cause a denial of service from the target

Figure 6 HTTP.sys attack traffic detected by the JSOC

The JSOC tested and confirmed that the response "416 Requested Range Not Satisfiable" was returned in response to the request of Figure 6a (Figure 7). The JSOC also confirmed that in response to the request of Figure 6b, the system displayed a blue screen and was restarted (Figure 8).

```
GET / HTTP/1.1
User-Agent: Wget/1.13.4 (linux-gnu)
Accept: */*
Host: 172.16.166.128
Connection: Keep-Alive
Range: bytes=0-18446744073709551615

HTTP/1.1 416 Requested Range Not Satisfiable
Content-Type: text/html
Last-Modified: Fri, 31 Jul 2015 15:21:20 GMT
Accept-Ranges: bytes
ETag: "60979c8da4cbd01:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Thu, 10 Sep 2015 14:41:14 GMT
Content-Length: 362
Content-Range: bytes */689

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Requested Range Not Satisfiable</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Requested Range Not Satisfiable</h2>
<hr><p>HTTP Error 416. The requested range is not satisfiable.</p>
</BODY></HTML>
```

Figure 7 Response if HTTP.sys had the vulnerability (test result)

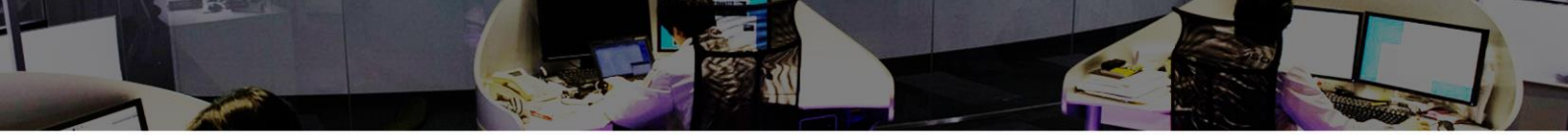


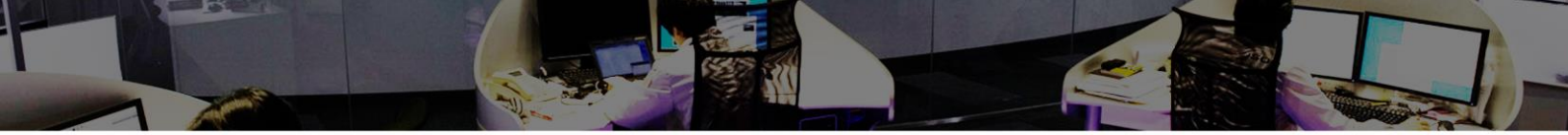
Figure 8 Server's blue screen as a result of attack traffic that exploits the vulnerability

In addition, it was also disclosed that the vulnerability remotely caused memory leakage from the content cache of the target. If the attack succeeds, the target would respond with memory contents. No detailed attack method has been disclosed, and as of September 1, 2015, the JSOC has not detected any attempt to exploit the vulnerability to obtain memory information. However, since an attack method that exploits the vulnerability easily may be disclosed, appropriate countermeasures should be taken as quickly as possible.

No attack code that allows command execution has been confirmed.

4.2.3 Countermeasures against the HTTP.sys vulnerability

The countermeasure for this vulnerability is to apply the program fix (MS15-034) available from Microsoft. If you use a system that may be affected, apply the program fix as quickly as possible.



4.3 Denial-of-service vulnerability in PHP

4.3.1 Overview of the denial-of-service vulnerability in PHP

The multipart_buffer_headers function of PHP has a defect in form-data file name handling. It has a vulnerability (CVE-2015-4024)[15, 16] that causes a denial of service condition due to a malicious HTTP request.

The PHP versions that may be affected by this vulnerability are as follows:

- PHP earlier than 5.4.41
- 5.5.x earlier than PHP 5.5.25
- 5.6.x earlier than PHP 5.6.9

As of September 1, 2015, the JSOC had not detected any attack traffic that exploited the vulnerability.

4.3.2 Testing attack traffic that exploited the vulnerability

Figure 9 shows an HTTP request used by the JSOC to test the vulnerability.

The test result showed that the CPU usage of the HTTP service increased when the HTTP request exploiting the vulnerability was received.

The effect of the vulnerability appears when the targeted file actually exists and performs PHP processing. If a directory is accessed without specifying a file, but if the host is configured to redirect access to the directory to a file that performs PHP processing, the attack will succeed by setting the directory as a target.

```
POST /index.php HTTP/1.1
Content-Length: 700195
Accept-Encoding: gzip, deflate
Connection: close
User-Agent: Mozillal/5.0 (Windows NT 6.1; WOW64) AppleWebKiti/537.36 (KHTML, like Gecko) Chromeu/40.0.2214.111 Safariss/537.36
Host: 10.1.11.21
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryX3B7rDMPcQlzmJE1

------WebKitFormBoundaryX3B7rDMPcQlzmJE1
Content-Disposition: form-data; name="file"; filename=sp.jpga
a
a
a
a
a
a
a
```

Figure 9 Part of an HTTP request in an attack that exploits the vulnerability for attacking (test result)

[15] JVNDB-2015-002263 in JVN iPedia vulnerability countermeasure information database - Denial-of-service (DoS) vulnerability in the PHP main / rfc1867.c multipart_buffer_headers function
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-003050.html

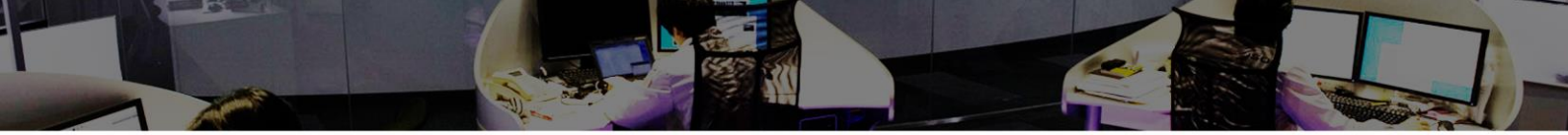
[16] php.net, Sec Bug #69364, PHP Multipart / form-data remote dos Vulnerability,
https://bugs.php.net/bug.php?id=69364

It has been confirmed that there is a tool specifically designed to attack the vulnerability as shown in Figure 10, and in the future, attack traffic is expected to occur.

Figure 10 Attack tool screen

4.3.3 Countermeasures against attacks that exploit the vulnerability

The countermeasure for the vulnerability is to apply a fixed version available from the vendor. If you use a system that may be affected, apply an appropriate program fix as quickly as possible.



5 Conclusion

Much like what the word "INSIGHT" itself implies, JSOC INSIGHT focuses on providing information on threats that our JSOC security analysts come across from time to time and believe to be worth noting.

Our security analysts are hard at work, carefully listening to customers in order to offer the most up-to-date information available. In our effort to provide vital information, the JSOC does not merely focus on the popular incidents that are discovered here and there, but also strives to draw attention to significant threats that can affect our now and tomorrow.

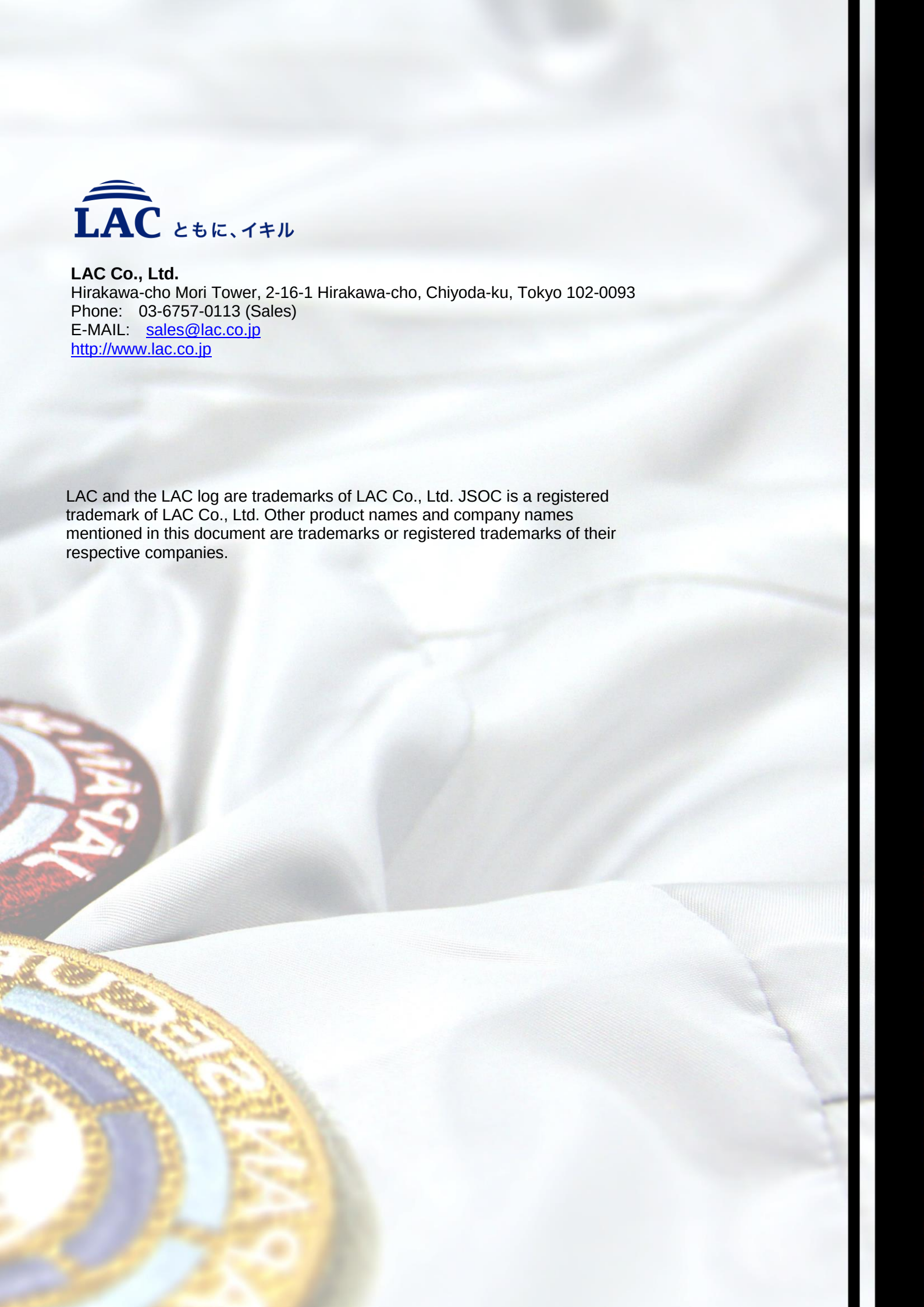
The JSOC's hope is to provide our customers with the safety and security that they need to conduct their business activities.

JSOC INSIGHT vol.9

Authors:

Shotaro Murakami, Yusuke Takai, Yuta Nisikino

(alphabetical order)



LAC Co., Ltd.
Hirakawa-cho Mori Tower, 2-16-1 Hirakawa-cho, Chiyoda-ku, Tokyo 102-0093
Phone: 03-6757-0113 (Sales)
E-MAIL: sales@lac.co.jp
http://www.lac.co.jp