株式会社ラック

INSIGHT

vol.9

2015 年 10 月 22 日

JSOC Analysis Team

JSOC JAPAN SECURITY OPERATION CENTER

JSOC INSIGHT Vol.9

JAPAN SECURITY OPERATION CENTER

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 4 月 1 日 ～ 2015 年 6 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。

※本文書の情報提供のみを目的としており、記述を利用した結果生じる、いかなる損失についても株式会社ラックは責任を負いかねます。
※本データをご利用いただく際には、出典元を必ず明記してご利用ください。
(例　出典：株式会社ラック【JSOC INSIGHT vol.9】)
※本文書に記載された情報は初回掲載時のものであり、閲覧・提供される時点では変更されている可能性があることをご了承ください。

2　エグゼクティブサマリ

本レポートは、2015 年 4 月から 6 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。

➢ 標的型攻撃によるマルウェア感染について

日本年金機構の情報漏えいで用いられたとされる、Emdivi と呼ばれるマルウェアに感染した通信を検知しております。感染通信を検知したお客様の業種・業態に偏りは見受けられず、多種の企業で感染を検知したのが特徴です。また、これまでのマルウェア検知の多くは海外の C&C サーバとの通信を行っていましたが、Emdivi に感染した端末の多くは日本のドメインをもつ C&C サーバとの通信をしていることも特徴にあげられます。また、Emdivi は国外ではほとんど感染事例がないことなどから、日本が攻撃の標的となっていると考えられます。

➢ HTTP.sys ファイル処理の脆弱性を悪用した攻撃通信を検知

Windows の特定バージョンに実装される Web サーバ(IIS)にサービス不能、および任意のコマンド実行を可能にする脆弱性が公開されました。非常に容易に本脆弱性を悪用し対象を再起動する手法が公開されており、JSOC では本手法による攻撃を検知しております。なお、コマンド実行を可能にする攻撃コードは確認しておりません。

➢ PHP に含まれるサービス不能の脆弱性について

PHP の特定のバージョンに、外部からサービス不能を引き起こす脆弱性が公開されました。本脆弱性を悪用する方法は非常に容易です。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、影響が大きいため、早急な対応が必要です。

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、2015 年 4 月から 6 月に発生した重要インシデントの件数推移を示します。

内部から発生した重要インシデントの発生件数は、4 月から 6 月は減少傾向にあり、6 月の発生件数は 4 月と比べ、約半数となりました。これは、3 月より継続してマルウェア感染を検知していた一部のお客様が 5 月末頃にインシデント対応を完了したためです。また、4 月 5 週および 6 月 1 週に複数のお客様で、標的型攻撃によるマルウェア感染と考えられる通信を検知しました(図 1-[1], [2])。

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 5 月 2 週～4 週に増加しました(図 1-[3])。これは、不正なファイルをアップロードする試みや SQL インジェクションなど、今までも検知していた攻撃による重要インシデントが増加したためです。

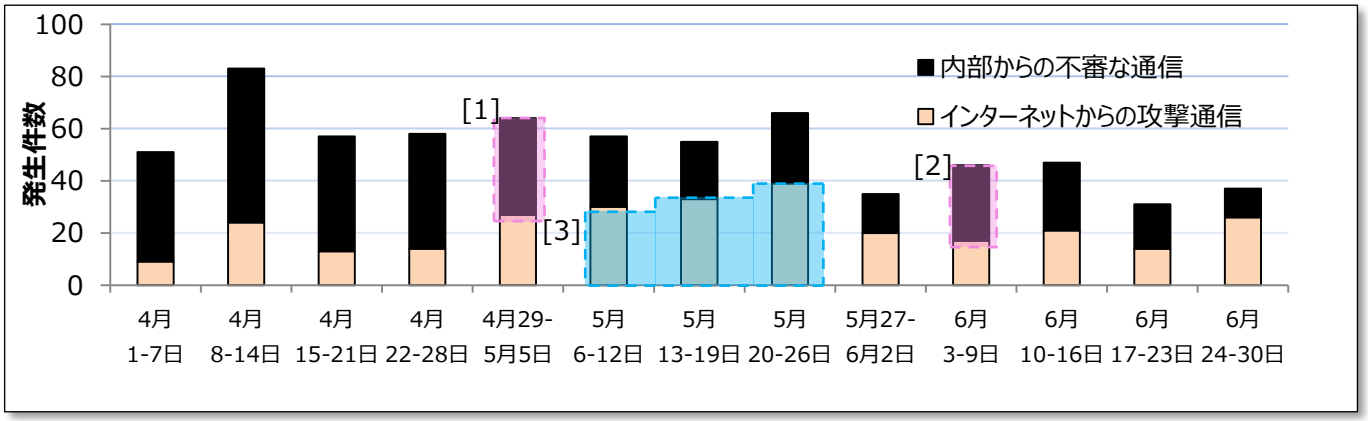


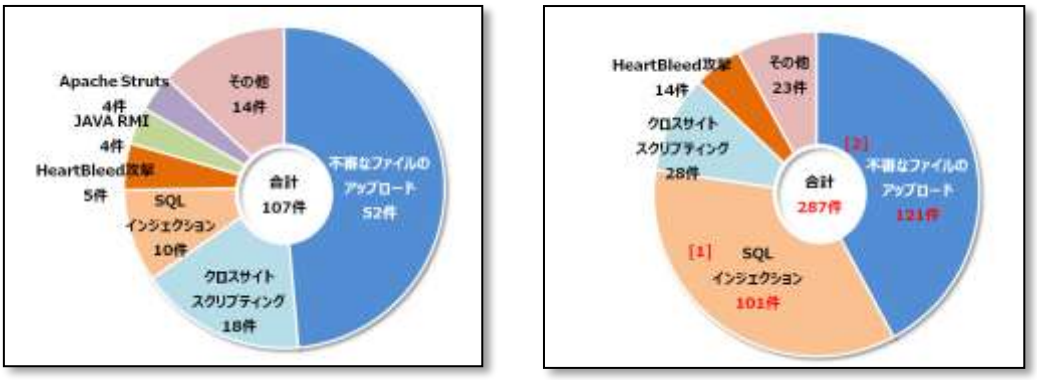
図 1 重要インシデントの発生件数推移(2015 年 4 月～6 月)

3.2　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4月から6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(287件)は、1月から3月の件数(107件)より大幅に増加しました。

これは、SQL インジェクションに脆弱なホストが存在したお客様に対し、同様の攻撃が繰り返し発生したためです(図 2 b-[1])。また、4月から6月には、WordPressのプラグインの脆弱性を悪用し、不審なファイルをアップロードする試みが無差別に行われ、重要インシデントが急増しました(図 2 b-[2])。



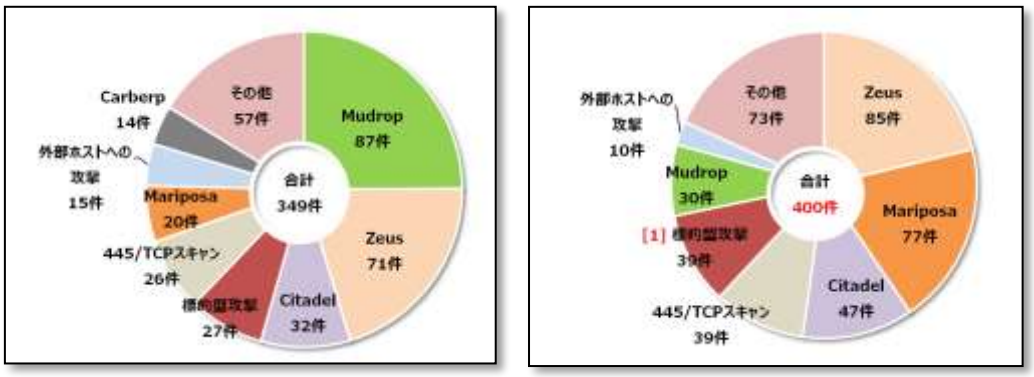
a. 2015 年 1～3 月　　**b. 2015 年 4～6 月**

図 2 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

図 3 に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4月から6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(400件)は、1月から3月の件数(349件)よりやや増加しました。これは、3月より、一部のお客様でマルウェア感染が継続したことに加え、Zeus/Zbotなどのインターネットバンキングの情報を狙ったマルウェア感染と考えられる通信を多く検知したためです。

また、サイバー救急センターの解析結果を元に、標的型攻撃の監視を強化した結果、2015年4月から6月に複数のお客様にて標的型攻撃によりマルウェアに感染した可能性のある通信を検知しました(図 3 b-[1])。



a. 2015 年 1～3 月　　**b. 2015 年 4～6 月**

図 3 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

3.3　大量に検知したインターネットからの攻撃通信例

表 2に2015年4月から6月における、インターネットからの攻撃通信で特に検知件数が多かった攻撃を示します。これらの攻撃通信の多くは、攻撃対象における特定のWebアプリケーションの利用有無にかかわらず無差別に行われており、その試みはほぼ失敗しております。しかしながら、攻撃対象の状況によっては大量の攻撃通信の発生がリソースの過度な消費につながる可能性もあります。

今期においては、このように攻撃通信が大量に発生することで分析コストが膨大になり、リアルタイム監視を行うJSOCアナリストをしばしば苦しめました。

表 2 大量に検知したインターネットからの攻撃通信

概要	JSOC の検知内容	検知時期	重要インシデントの有無
Shellshock の検知	Shellshock[1]の脆弱性有無を調査する通信や、ホストの悪用を試みる攻撃を継続して検知しました。攻撃に用いられるコマンドは多岐にわたりました。	2015 年 5 月上旬まで	無
phpMoAdmin に対する攻撃	phpMoAdmin に対するコマンド実行の試み[2]を検知しました。攻撃に用いられたコマンドは攻撃対象のホスト情報の表示を試みる内容でした。	2015 年 6 月上旬	無
OpenView NNM に対する攻撃	HP 社の製品「OpenView NNM」の脆弱性[3]を悪用し、コマンドを実行する試みを検知しました。攻撃の送信元ホストは 1 台から、存在するすべての IPv4 アドレスに対して攻撃を実施しているように見受けられました。	2015 年 6 月中旬	有
WordPress に対する脆弱性スキャン	WordPress のプラグインの脆弱性を悪用し、設定ファイルを閲覧する試みや不正なファイルをアップロードする試みを検知しました。	決まった時期は無く、定常的に検知	有

[1] JSOC INSIGHT vol. 7
4.1 Shellshock の検知傾向変化について
http://www.lac.co.jp/security/report/pdf/20150519_jsoc_m001t.pdf

[2] JSOC INSIGHT vol. 8
3.2 phpMoAdmin におけるコード実行の脆弱性について
http://www.lac.co.jp/security/report/pdf/20150713_jsoc_j001m.pdf

[3] HP サポートドキュメント - HP サポートセンター（ドキュメント ID: c02215897）
http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c02215897

4　今号のトピックス

4.1　標的型攻撃によるマルウェア感染について

JSOC は、緊急対応チーム「サイバー救急センター」と連携し、新たな攻撃手法や事例を相互に情報共有しています。サイバー救急センターから提供された標的型攻撃やマルウェア感染の情報を元に、対応が可能なものは JSOC オリジナルシグネチャ(JSIG)を作成します。これにより、IDS・IPS メーカから提供されるシグネチャ群では対応できない不審な通信への対応や、特に日本の政府機関や企業を狙うことに特化した標的型攻撃などに対応し、検知可能な範囲を広げています。

2015 年４月から７月に、JSOC で監視中の複数のお客様にて標的型攻撃によるマルウェアに感染した通信を検知し、緊急連絡を行いました。これらの事例には、日本年金機構の情報漏えい[4]で用いられたとされる、「Emdivi」と呼ばれるマルウェア通信の検知も含まれております。

4.1.1 Emdivi に感染した通信の検知事例

図 4 に Emdivi による重要インシデントの発生件数推移を示します。

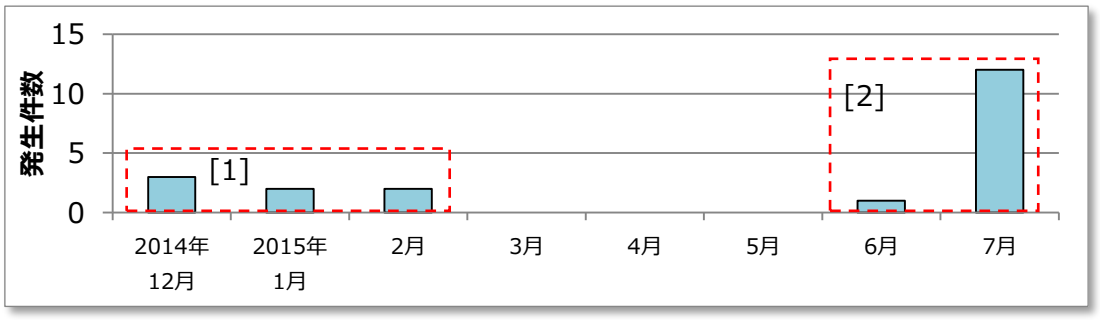


図 4　Emdivi による重要インシデントの件数推移

JSOC では、Emdivi の感染通信を 2014 年 12 月から 2015 年 2 月に標的型攻撃の一種として検知しました(図 4-[1])。その後、6 月末までは検知がありませんでしたが、6 月末以降 Emdivi に感染したと考えられる通信を複数のお客様で検知しました(図 4-[2])。

Emdivi は、標的型メールに添付されたファイルをユーザ自身が開封することや、改ざんされた Web サイトを閲覧し、不正なファイルをダウンロードするドライブバイダウンロード攻撃によって感染します。Emdivi に感染した端末が外部の C&C サーバに接続することで、攻撃者が感染端末をリモートから操作することが可能となります。

[4]日本年金機構における不正アクセスによる情報流出事案について
http://www.mhlw.go.jp/kinkyu/150603.html

2014 年 11 月にジャストシステムから一太郎シリーズにおいて任意のコードが実行される脆弱性[5]が公開され、当時の感染通信の検知は、標的型メールに添付された本脆弱性を悪用するファイルを実行したことによる可能性があります。一太郎は日本国内での利用がほとんどであり、日本を対象とした攻撃であることが考えられます(図 4-[1])。

JSOC では 3 月から 6 月中旬まで Emdivi の検知はありませんでしたが、サイバー救急センターでは、お客様からの依頼が 2015 年に入って急増し、Emdivi に感染した事例を確認しました[6]。これらの傾向から、攻撃者による感染フェーズが終わり、感染端末からの情報取得フェーズに移った可能性が考えられます。

日本年金機構は 6 月 1 日に、約 125 万件の基礎年金番号を含む個人情報が漏えいしたことを発表しました。本件は公的機関からの情報漏えいとしては過去最大であり、標的型攻撃に関する大きな注目を集め、様々な機関や企業が本事件に関するレポート[7]を公開しました。また、8 月 20 日に日本年金機構及び内閣サイバーセキュリティセンター(NISC)から本事件に関する調査結果[8,9]が公開され、翌 21 日には厚生労働省から本事件に関する検証報告書[10]が公開されました。

JSOC では 6 月下旬以降、Emdivi に感染した通信の検知が増加しております(図 4-[2])。これらの感染通信を検知したお客様に業種・業態などによる傾向は見受けられず、さまざまな業種のお客様に無差別に攻撃が行われたと考えられます。

図 5 に Emdivi に感染した通信の検知例を示します。

Emdivi に感染した端末からは GET リクエストおよび POST リクエストによる通信が発生します。GET リクエストによる通信は、Cookie ヘッダに感染端末の情報を含みます。また、POST リクエストによる通信は、「index.php」や、「/15932?p=#」のような「/ランダムな数字?p=#」の URI に対して、データ部分に感染端末の情報を含む通信を検知しています。

---

[5] 一太郎の脆弱性を悪用した不正なプログラムの実行危険性について
http://www.justsystems.com/jp/info/js14003.html

[6] 水面下で侵攻するサイバースパイ活動急増に関する注意喚起
http://www.lac.co.jp/security/alert/2015/06/16_alert_01.html

[7] 「日本年金機構の情報漏えい事件から得られる教訓」公開のお知らせ
http://www.lac.co.jp/news/2015/06/09_news_01.html

[8] 不正アクセスによる情報流出事案に関する調査結果について
https://www.nenkin.go.jp/oshirase/press/2015/201508/20150820-02.files/press0820.pdf

[9] 日本年金機構における個人情報流出事案に関する原因究明調査結果
http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf

[10] 日本年金機構における不正アクセスによる情報流出事案検証委員会検証報告書
http://www.mhlw.go.jp/kinkyu/dl/houdouhappyou_150821-02.pdf

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

▲：感染端末のホスト名と動作しているプロセスIDを難読化した文字列
■：何らかの情報を難読化した文字列
```

(a) GET リクエストによる通信

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

[ランダムな文字列]=▲▲▲&date= ■ ■ ■

▲：感染端末のホスト名と動作しているプロセスIDを難読化した文字列
■：何らかの情報を難読化した文字列
```

(b) POST リクエストによる通信(index.php あて)

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

[ランダムな文字列]=▲▲▲&date= ■ ■ ■

▲：感染端末のホスト名と動作しているプロセスIDを難読化した文字列
■：何らかの情報を難読化した文字列
```

(c) POST リクエストによる通信(/ランダムな数字?p=#あて)

図 5 Emdivi に感染した端末からの通信例

表 3 に、JSOC で検知した Emdivi 感染端末から発生した通信の接続先を示します。

JSOC では、これまで標的型攻撃などマルウェアに感染したホストから C&C サーバへの接続通信は、海外に設置されたホストへの検知が大部分を占めていました。しかしながら、Emdivi に感染したホストから発生した通信の特徴は、表 3 に示すとおり日本のドメインをもつ C&C サーバへ通信しています。また、これらの接続先となった C&C サーバは、特定のクラウドサービスを提供する会社が管理する Web サイトが多数を占めました。これらの Web サイトではブログなどを中心に正規の Web コンテンツが稼動しておりましたが、特定の Web アプリケーションを利用しているわけではありませんでした。このことから攻撃者は特定の Web アプリケーションの脆弱性を攻撃しホストを悪用した可能性は低いものの、明確な手法は不明です。感染ホストから C&C サーバへの通信をネットワーク機器などで遮断されないよう、日本国内で利用されているホストを悪用したと考えます。

これらの状況から、Emdivi による標的型攻撃は日本に特化した形で行われ、日本のユーザが攻撃の対象となっていると考えます。

表 3 JSOC で検知した Emdivi に感染した端末から発生した通信の接続先

接続先IPアドレス	接続先ドメイン名	国
125.XXX.XXX.72	www. .co.jp www. .com www. .co.jp	日本
125.XXX.XXX.79	www. .com www. .co.jp	
125.XXX.XXX.113	www. .com www. . .org	
125.XXX.XXX.114	www. .com	
203.XXX.XXX.233	www. .jp	
54.XXX.XXX.0	www. .co.jp	米国
—	www. .co.jp	
103.XXX.XXX.59	—	香港
203.XXX.XXX.210	www. .com	
—	www. .com	不明

4.1.2 Emdivi などの標的型攻撃への対策

標的型攻撃の手法は巧妙化しており、個人が意識して行う対策に加え、組織として標的型攻撃に対する訓練の実施や、事故発生を前提としたインシデントレスポンス体制の整備など複合的な対策が必要です。[11,12]

■ 組織としての対策

・定期的な社員教育
・最新の脅威情報などの収集
・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
・不審なメールおよび添付ファイルは開かない
・Mircosoft 社が提供する EMET を導入する(被害の軽減策)

■ 運用者としての対策

・ウイルス対策ソフトを導入する
・ファイアウォール、次世代ファイアウォール、IDS、IPS、MPS などのセキュティデバイスによる防御
・実行ファイルが添付されたファイルをシステム的に破棄する
・SPF（Sender Policy Framework）による送信元ドメインの確認

また、万一インシデントが発生した場合に備え、事後の調査を可能にするため、セキュティデバイス、プロキシサーバやメールサーバなどアウトバウンド通信のログを取得することが重要となります。

---

[11]日本年金機構の情報漏えい事件から、我々が得られる教訓
http://www.lac.co.jp/security/report/pdf/20150609_apt_j001t.pdf
[12]日本年金機構の事件報告を受けて、なすべき最低限の対策について
http://www.lac.co.jp/security/report/pdf/20150831_apt_a001m.pdf

4.2 HTTP.sys ファイル処理の脆弱性を悪用した攻撃通信の検知について

4.2.1 HTTP.sys の脆弱性について

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)に、リモートから任意のコード実行が可能な脆弱性(CVE-2015-1635、MS15-034)が公開されました。これは、HTTP リクエストの解析処理に不備があり、悪意のある Range ヘッダを含むリクエストの処理に起因してサービス不能状態や、コンテンツキャッシュのメモリリークが発生する脆弱性です。[13,14]

本脆弱性の影響を受ける可能性があるのは、MS15-034 が未適用で IIS を有効化した表 4 のソフトウェアです。

表 4 HTTP.sys の脆弱性の影響を受ける可能性のあるソフトウェア一覧

ソフトウェア	バージョン	エディション
Microsoft Windows	7	32-bit Systems SP1
		x64-based Systems SP1
	8	32-bit Systems
		x64-based Systems
	8.1	32-bit Systems
		x64-based Systems
Microsoft Windows Server	2008 R2	Itanium-Based Systems SP1
		x64-based Systems SP1 (Server Core インストール含む)
	2012	Server Core インストール含む
	2012 R2	Server Core インストール含む

4.2.2 JSOC における HTTP.sys の脆弱性を狙った攻撃の検知事例

図 6 に JSOC で検知した本脆弱性を悪用する通信を示します。

JSOC では攻撃対象の脆弱性の有無を調査する通信(図 6.a)や、脆弱性を悪用し攻撃対象を再起動させる攻撃通信(図 6.b)を検知しております。これらの通信において異なる点は、HTTP リクエストと Range ヘッダで指定する範囲の開始値であり、内容によって攻撃による影響が異なります。

---

[13]セキュリティ TechCenter、 マイクロソフト セキュリティ情報 MS15-034 – 緊急
https://technet.microsoft.com/ja-jp/library/security/ms15-034.aspx
[14]複数の Microsoft Windows 製品の HTTP.sys における任意のコードを実行される脆弱性
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-002263.html

```
Stream Content
GET / HTTP/1.1
Host: [redacted]
Range: bytes=0-18446744073709551615
```

(a) HTTP.sys の脆弱性の有無を調査する通信

```
Stream Content
GET /welcome.png HTTP/1.0
User-Agent: Wget/1.11.4
Accept: */*
Host: [redacted]
Connection: Keep-Alive
range: bytes=18-18446744073709551615
```

(b) HTTP.sys の脆弱性を悪用して攻撃対象にサービス不能を起こす攻撃

図 6 JSOC で検知した HTTP.sys の攻撃通信

JSOC でこれらのリクエストを検証したところ、図 6.a のリクエストに対し、「416 Requested Range Not Satisfiable」の応答を確認しました(図 7)。図 6.b のリクエストに対しては、ブルースクリーン状態となり再起動することを確認しました(図 8)。

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

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

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

図 7 HTTP.sys の脆弱性が存在する場合の応答内容(検証結果)

図 8 本脆弱性を悪用した攻撃通信によりブルースクリーン状態となったサーバの表示画面

また、本脆弱性により、リモートから攻撃対象のコンテンツキャッシュのメモリリークが発生することが公開されています。攻撃が成功すると、攻撃対象はメモリの内容を含んで応答します。なお、詳細な攻撃手法は公開されておらず JSOC では 2015 年 9 月 1 日現在まで、本脆弱性を悪用しメモリの情報を取得する試みは検知しておりませんが、容易に脆弱性を悪用する手法が公開される可能性があるため、早急な対策が必要です。

なお、コマンド実行を可能にする攻撃コードは確認しておりません。

4.2.3 HTTP.sys の脆弱性対策

本脆弱性への対策は Microsoft 社が提供する修正プログラム(MS15-034)を適用することです。影響を受ける可能性のあるシステムを利用している場合は、可能な限り早急に修正プログラムの適用による対応を行うことを推奨します。

4.3 PHP に含まれるサービス不能の脆弱性について

4.3.1 PHP に含まれるサービス不能の脆弱性の概要

PHP の multipart_buffer_headers 関数には、form-data のファイル名の取り扱いに不備があり、悪意のあるHTTPリクエストによりサービス不能状態に陥る脆弱性(CVE-2015-4024)[15,16]が存在します。

本脆弱性の影響を受ける可能性のあるバージョンは以下のとおりです。

- PHP 5.4.41 未満
- PHP 5.5.25 未満の 5.5.x
- PHP 5.6.9 未満の 5.6.x

2015 年 9 月 1 日現在、JSOC では本脆弱性を悪用する攻撃通信は確認しておりません。

4.3.2 本脆弱性を悪用した攻撃通信の検証

図 9 に JSOC で本脆弱性の検証を行った際の HTTP リクエストを示します。

検証の結果、脆弱性を悪用した HTTP リクエストを受信すると、HTTP サービスの CPU 使用率が上昇することを確認しました。

本脆弱性の影響を受ける条件は、攻撃対象のファイルが実際に存在し、そのファイルが PHP の処理を行うことです。ファイルを指定せずにディレクトリアクセスした際でも PHP 処理を行うファイルに転送するよう設定されたホストでは、そのディレクトリを攻撃対象としても攻撃は成功します。

```
POST /index.php HTTP/1.1
Content-Length: 700195
Accept-Encoding: gzip, deflate
Connection: close
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.111 Safari/537.36
Host: 10.1.11.21
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryX387rDWPcQlzmJE1

------WebKitFormBoundaryX387rDWPcQlzmJE1
Content-Disposition: form-data; name="file"; filename=sp.jpga
a
a
a
a
a
a
a
```

図 9 本脆弱性を悪用する攻撃の HTTP リクエストの一部(検証結果)

---

[15] JVN iPedia 脆弱性対策情報データベース、 JVNDB-2015-002263、 PHP の main / rfc1867.c の multipart_buffer_headers 関数におけるサービス運用妨害 (DoS) の脆弱性
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-003050.html

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

また、図 10 へ示す本脆弱性を狙った攻撃専用のツールが存在していることを確認しており、今後攻撃通信が発生する可能性があります。

図 10 攻撃ツール画面

4.3.3 本脆弱性を悪用した攻撃への対策

本脆弱性への対策はメーカが公開する修正バージョンを適用することです。影響を受ける可能性のあるシステムを利用している場合は、可能な限り早急に修正プログラムの適用による対応を行うことを推奨します。

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.9
【執筆】
高井　悠輔　/錦野　友太/　村上　正太郎
(五十音順)

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