Distributed via
@police
http://www.npa.go.jp/cyberpolice/

平成 29 年 12 月 19 日

Topic

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

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しました。これらに関連して、ロジテック株式会社は同社が販売するブロードバンドルータの脆弱性及びその対策について注意喚起しています。該当製品の利用者は適切な対策を早急に実施することを推奨します。

1 脆弱性が存在するルータを標的とした 52869/TCP に対するアクセスの観測

警察庁の定点観測システムにおいて、平成 29 年 11 月1日から宛先ポート 52869/TCP に対するアクセスの増加を観測しました(図1)。

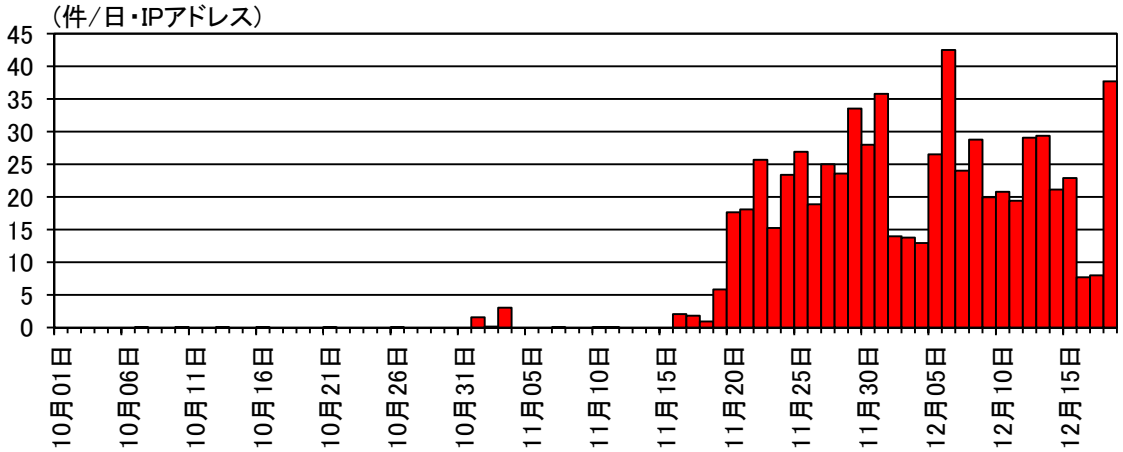

図1 宛先ポート 52869/TCP に対するアクセス件数の推移(H29.10.1～12.18)

観測したアクセスの内容を確認したところ、細工された SOAP[i] リクエストになっており、外部のウェブサイトからファイルをダウンロードするコマンド等が挿入されていました(図2)。

[i] Simple Object Access Protocol の略であり、プログラム同士がネットワークを通じて情報交換するための通信プロトコルの一種。メッセージの記述に XML を使用し、データ伝送には主に HTTP が使用される。

図2　宛先ポート 52869/TCP に対するアクセスの観測例（一部をマスキング）

当該アクセスは、その特徴から Realtek 社が提供する SDK を使用して製造された特定のルータに存在する脆弱性[i]を悪用し、不正にコマンドを実行する目的であると考えられます。脆弱性が存在し、ファイルのダウンロードが成功した機器に対しては、引き続きダウンロードしたファイルを実行するコマンドが送信されるものと考えられます。このことから、攻撃者は脆弱性が存在する機器に対して、不正プログラムの感染拡大を図っているものと推測されます。

2　日本国内からの Telnet による探索を実施するアクセスの急増

宛先ポート 52869/TCP に対するアクセスの増加と同時期に、日本国内に割当てられた IP アドレスを発信元とする宛先ポート 23/TCP 及び 2323/TCP に対するアクセスの急増を観測しました（図3）。23/TCP は Telnet で使用されるポートであり、2323/TCP についても一部の機器において同様の目的で使用されています。このことから、Telnet により外部からアクセス可能な機器の探索が実施されているものと考えられます。

なお、同ポートに対するアクセスについては、日本国外に割り当てられた IP アドレスからは顕著な増加は見られませんでした。

[i] 「Realtek SDK の miniigd SOAP サービスにおける任意のコードを実行される脆弱性」
http://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-008039.html

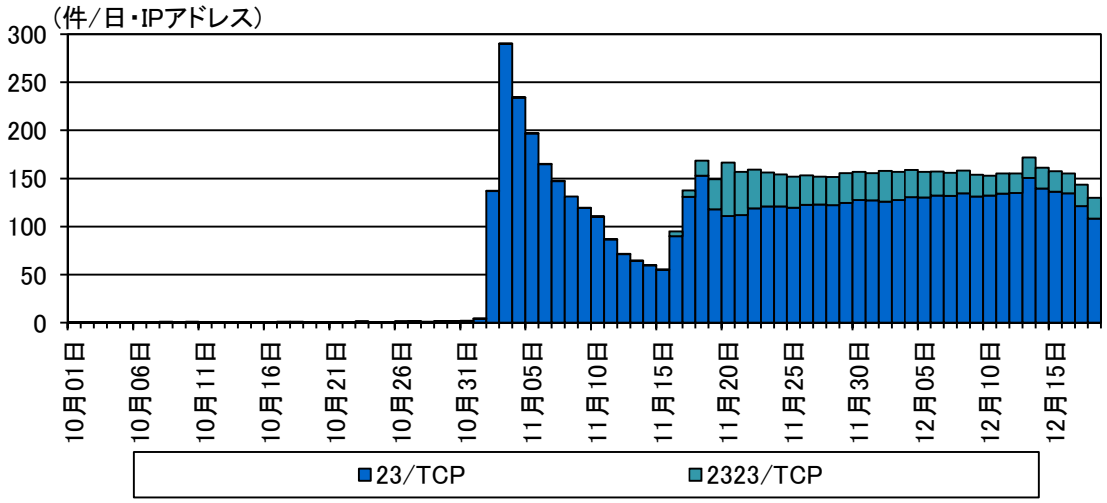

図3　日本国内からの宛先ポート 23/TCP 及び 2323/TCP に対するアクセス件数の推移
（H29.10.1～12.18）

当該アクセスの大多数は、宛先 IP アドレスと TCP シーケンス番号[i]の初期値が一致しており、IoT 機器に感染する Mirai ボット[ii]の特徴を有していました。このことから、これらのアクセスは Mirai ボットのソースコードを流用して作成された不正プログラムが、新たな感染対象を探索する活動であると推測されます。

また、当該アクセスの発信元 IP アドレスを調査すると、外部から 52869/TCP 及び 52881/TCP の各ポートにアクセス可能なものが多数確認できました。発信元 IP アドレスの同ポートに対する調査により得られた結果には、Realtek 社の名称や「Wireless Router」との名称が含まれていたことから、Realtek 社が提供する SDK を使用して製造された無線 LAN 機能が付属したルータが発信元となっているものと推測されます。

これらの状況から、日本国内の脆弱性が存在するルータが、脆弱性を悪用した 52869/TCP に対する攻撃を受けて、Mirai ボットのソースコードを流用して作成された不正プログラムに感染し、23/TCP 及び 2323/TCP ポートに対して新たな感染対象を探索する活動を実施している可能性が考えられます。

---

[i] TCP パケットの送受信状況を管理するために付与される番号。通常は TCP 通信の開始時にランダムな番号が初期値として設定され、TCP 通信の進行に合わせて増加する。また、この初期値を特に ISN（Initial Sequence Number）という。

[ii] 「インターネット観測結果等（平成 28 年）」の「IoT 機器を標的とする「Mirai」ボットの探索行為及び感染活動」を参照
https://www.npa.go.jp/cyberpolice/important/2017/201703231.html

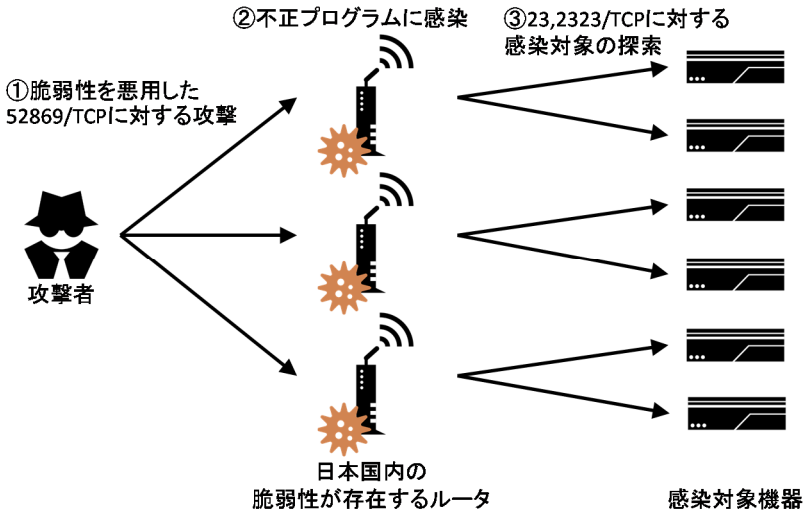

図5　実施されていると予想される攻撃の流れ

3　ロジテック社製ルータに存在する脆弱性及び推奨する対策について

ロジテック株式会社は同社が販売する以下のブロードバンドルータ及びセットモデル（全 11 モデル）に関し、1で述べた脆弱性の影響を回避する修正済みのファームウエアを 2013 年 6 月より順次公表していましたが、12 月 19 日に改めて利用者に対し対策を呼び掛けています[i]。また、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）[ii]、国立研究開発法人情報通信研究機構（NICT）[iii]等からも本件について同日に注意喚起が実施されています。

- LAN-WH300N/DR　Ver2.14 より前
- LAN-W300N/DR　　Ver2.14 より前
- LAN-WH300N/DRCV　　Ver2.14 より前
- LAN-WH300N/DRCY　　Ver2.14 より前
- LAN-W300N/R　　Ver2.33 より前
- LAN-W300N/RU2　　Ver2.33 より前
- LAN-W300N/RS　　Ver2.33 より前
- LAN-W300N/P　　Ver3.09 より前
- LAN-W300N3L　　Ver1.13N3L より前
- LAN-WH300N/DGR　　Ver1.26 より前
- LAN-WH300N/DGRU　　Ver1.26 より前

2で述べた、観測された Telnet による探索を実施するアクセスの発信元と考えられる日本国内の不正プログラムに感染したルータには、今回公表されたロジテック社製のブロードバンドルータ、

[i] 「ロジテック社製 300Mbps 無線 LAN ブロードバンドルータ及びセットモデル（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

[ii] 「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

[iii] 「IoT 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）」
http://www.nicter.jp/report/2017-01_mirai_52869_37215.pdf

又はセットモデルが含まれている可能性があります。このため、以下の対策を早急に実施することを強く推奨します。

- ロジテック社等が公表する情報を参照し、当該機種を使用していないか確認してください。
- 当該機種を使用していた場合には、使用しているファームウェアが下記の修正済みのバージョンになっていることを確認してしてください。

- LAN-WH300N/DR	Ver2.14	(2014 年 6 月 11 日公開)
- LAN-W300N/DR	Ver2.14	(2014 年 6 月 11 日公開)
- LAN-WH300N/DRCV	Ver2.14	(2014 年 6 月 11 日公開)
- LAN-WH300N/DRCY	Ver2.14	(2014 年 6 月 11 日公開)
- LAN-W300N/R	Ver2.33	(2013 年 11 月 6 日公開)
- LAN-W300N/RU2	Ver2.33	(2013 年 11 月 6 日公開)
- LAN-W300N/RS	Ver2.33	(2013 年 11 月 6 日公開)
- LAN-W300N/P	Ver3.09	(2014 年 8 月 22 日公開)
- LAN-W300N3L	Ver1.13N3L	(2013 年 6 月 25 日公開)
- LAN-WH300N/DGR	Ver1.26	(2014 年 10 月 15 日公開)
- LAN-WH300N/DGRU	Ver1.26	(2014 年 10 月 15 日公開)

- 脆弱性が存在するバージョンのファームウェアを使用していた場合には、ロジテック社が提供している修正済みファームウェアへの更新を速やかに実施してください。

また、当該脆弱性の影響を受ける機器は、ロジテック社が販売する当該機種以外にも多数存在するものと考えられます。当該機種を使用していない場合にあっても、以下の対策を実施することを推奨します。

- 特にインターネット上から直接アクセスされる可能性があるルータ等の機器について、利用している機種と、製造元又は貸与元(ISP 事業者等)を確認してください。
- 製造元又は貸与元が公表する当該機器に関する脆弱性情報や、その対応策を確認して、必要であれば対応を実施してください。
- 製造終了から年月が経過して、製造元の対応が終了している製品については、新しい製品への交換を検討してください。