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

レポート

平成 30 年6月 29 日

# GPON ルータの脆弱性を標的としたアクセスの観測等について

- GPON ルータの脆弱性を標的としたアクセスの観測
- 「Realtek SDK」の脆弱性（CVE-2014-8361）を標的とした宛先ポート 52869/TCP に対するアクセスの増加

## 1 GPON ルータの脆弱性を標的としたアクセスの観測

平成 30 年4月 30 日に、深刻な脆弱性（CVE-2018-10561 及び CVE-2018-10562 [i] ）を有する GPON [ii] を利用したルータ（以下「GPON ルータ」という。）がインターネット上に多数存在していることを海外 IT 企業が公表 [iii] しました。当該脆弱性は、HTTP リクエストに特定の文字列を挿入することで攻撃が可能となるもので、当該脆弱性が悪用された場合、認証を回避し、遠隔からコードを実行させることが可能であるとされています。

警察庁の定点観測システムにおいては、5月6日頃から当該脆弱性を標的としたアクセスを観測しました（図1）。

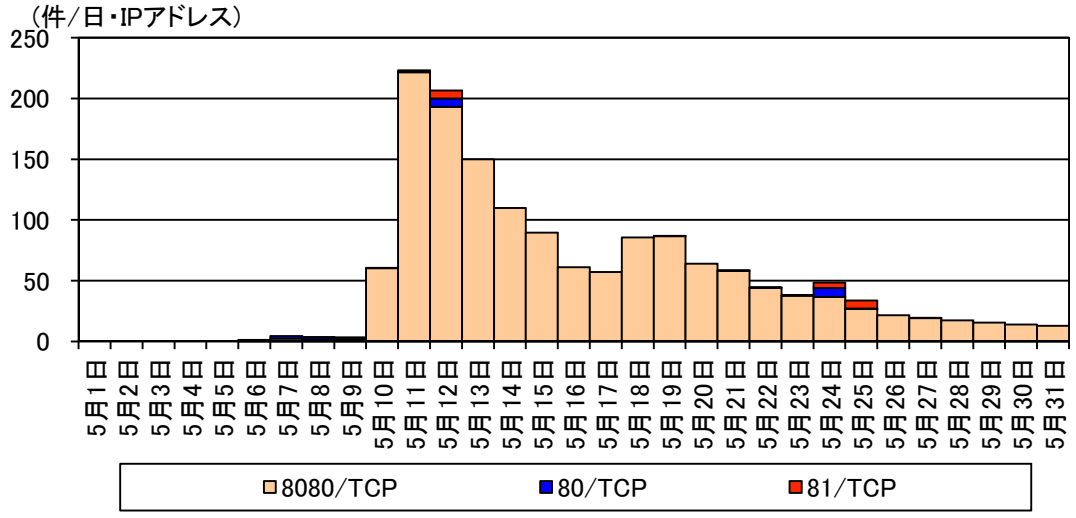


図1 GPON ルータの脆弱性を標的としたアクセス件数の推移（宛先ポート別）

[i] 「CVE-2018-10561 Detail」
https://nvd.nist.gov/vuln/detail/CVE-2018-10561
「CVE-2018-10562 Detail」
https://nvd.nist.gov/vuln/detail/CVE-2018-10562

[ii] Gigabit Passive Optical Network の略。1本の光ファイバーを分岐し、複数の利用者で共有する伝送技術の一つです。

[iii] 「Critical RCE Vulnerability Found in Over a Million GPON Home Routers」
https://www.vpnmentor.com/blog/critical-vulnerability-gpon-router/

観測したアクセスの多くは、当該脆弱性を悪用し、外部サーバから不正プログラムのダウンロード及び実行を試みるものでした（図2）。


図2　観測したアクセスの例（一部をマスキング）

当該アクセスの発信元を調査したところ、GPON ルータ、デジタルビデオレコーダ等の IoT 機器のログイン画面が表示されることを確認しました。

また、発信元を国・地域別で見た場合、メキシコを発信元とするものがほとんどであり、国内を発信元とするアクセスは観測されませんでした（図3）。

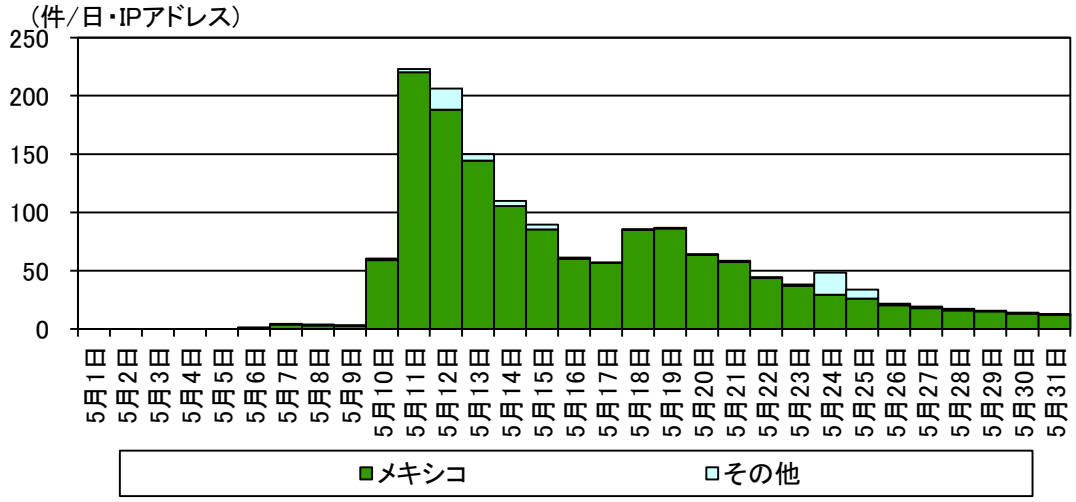


図3　GPON ルータの脆弱性を標的としたアクセス件数の推移（発信元国・地域別 [i] ）

[i] 発信元の国・地域については、当該国・地域に割り当てられた IP アドレスを指しています。以降も同様の表記です。

さらに、同発信元からは、仮想通貨採掘ソフトウェア「Claymore」を標的とした 3333/TCP へのアクセスや特定のファイルのダウンロード及び実行を試みる 52869/TCP へのアクセス [i] なども観測しています。

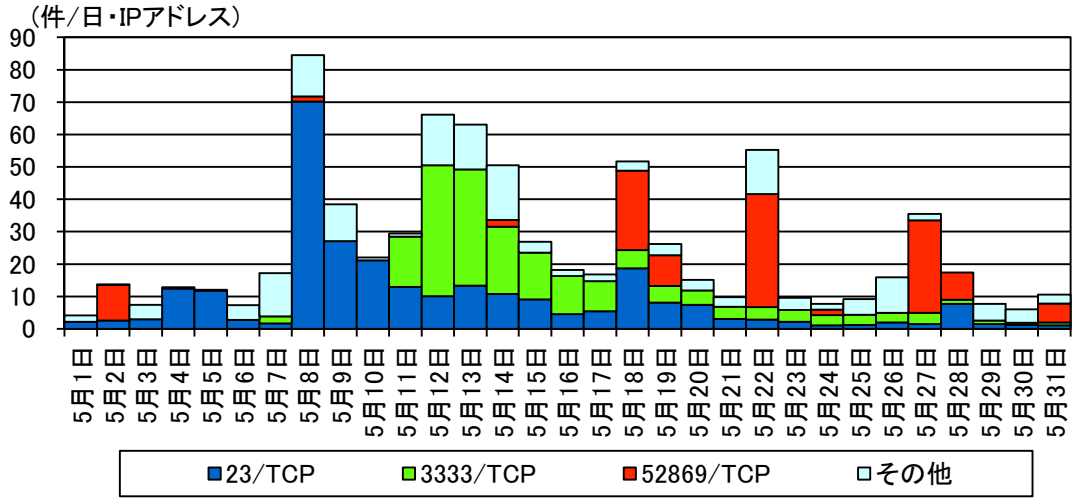


**図4　GPON ルータの脆弱性を標的としたアクセスの同一発信元からのアクセス件数の推移**
**（宛先ポート別　8080/TCP、80/TCP 及び 81/TCP を除く）**

このようなことから、GPON ルータをはじめとする IoT 機器に感染したボットが行った、感染拡大や仮想通貨採掘のための、脆弱な機器の探索行為を観測したものと考えられます。また、海外セキュリティベンダーによるレポートにおいても、数種類のボットが当該脆弱性を悪用して感染活動等を行っているなど、今回の観測されたものと同様な状況が報告 [ii] されています。

---

[i] 「仮想通貨採掘ソフトウェア「Claymore（クレイモア）」を標的としたアクセスの増加等について」
https://www.npa.go.jp/cyberpolice/important/2018/201803121.html

[ii] 「GPON Exploit in the Wild (I) – Muhstik Botnet Among Others」
https://blog.netlab.360.com/gpon-exploit-in-the-wild-i-muhstik-botnet-among-others-en/
「GPON Exploit in the Wild (II) – Satori Botnet」
http://blog.netlab.360.com/gpon-exploit-in-the-wild-ii-satori-botnet-en/
「GPON Exploit in the Wild (III) – Mettle, Hajime, Mirai, Omni, Imgay」
http://blog.netlab.360.com/untitled-3gpon-exploit-in-the-wild-iii-mettle-hajime-mirai-omni-imgay-en/
「GPON Exploit in the Wild (IV) – TheMoon Botnet Join in with a 0day(?)」
http://blog.netlab.360.com/gpon-exploit-in-the-wild-iv-themoon-botnet-join-in-with-a-0day/

## ２ 「Realtek SDK」の脆弱性（CVE-2014-8361）を標的とした宛先ポート 52869/TCP に対するアクセスの増加

警察庁の定点観測システムにおいて、平成 30 年5月中旬から下旬にかけて「Realtek SDK」の脆弱性（CVE-2014-8361）を標的とした宛先ポート 52869/TCP に対するアクセス（以下「「Realtek SDK」の脆弱性を標的としたアクセス」という。）の増加を観測しました（図5）。

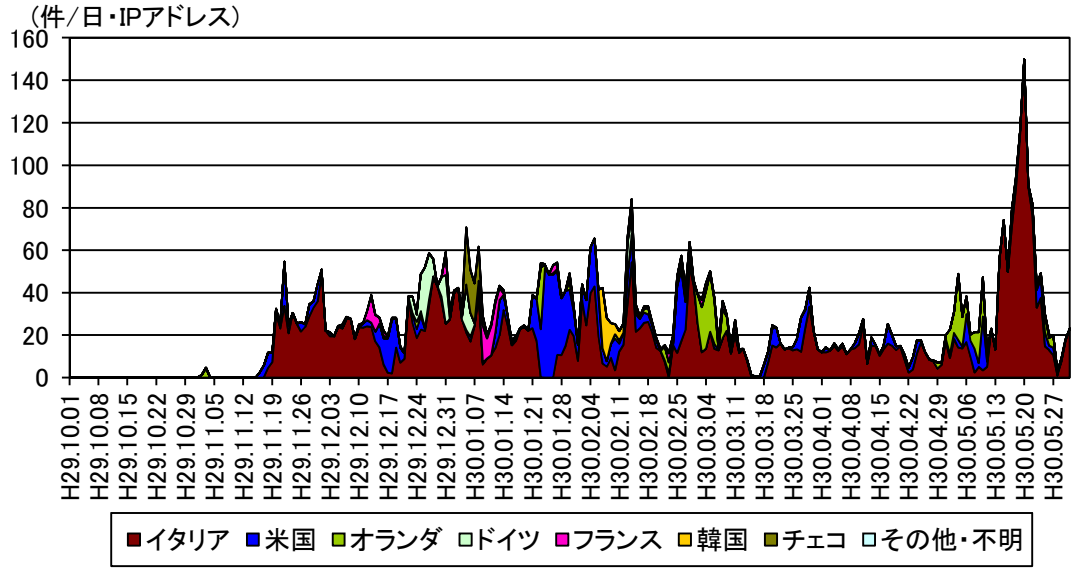


図５ 「Realtek SDK」の脆弱性を標的としたアクセス件数の推移
（発信元国・地域別 H29.10.1～H30.5.31）

当該アクセスについては、平成 29 年 11 月から継続的に観測しており、同年 12 月 19 日に注意喚起[i]を実施しています。

観測したアクセスは、細工された SOAP[ii] リクエストに対して、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や同ファイルを実行するコマンド等が挿入されているものでした（図6）。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機器に存在する脆弱性[iii]を悪用して不正にコマンドを実行し不正プログラムの感染拡大を図っているものと考えられます。

---

[i] 「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」（平成 29 年 12 月 19 日）
https://www.npa.go.jp/cyberpolice/important/2017/201712191.html

[ii] 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 が使用されます。

[iii] 「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6 「Realtek SDK」の脆弱性を標的としたアクセスの観測例（一部をマスキング）

また、5 月中旬には、Mirai ボットの亜種によるアクセス[i]と発信元 IP アドレスが同じアクセスも併せて観測されました（図7）。Mirai ボットの亜種に感染した機器を用いて不正プログラムの感染拡大を図っていた可能性があります。

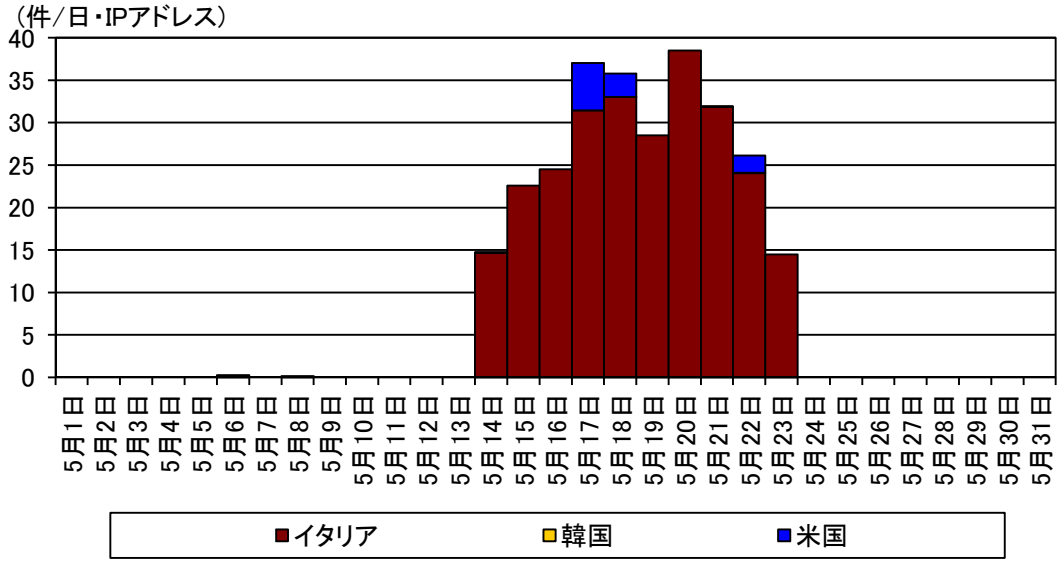


図7 Mirai ボットの亜種に感染した機器からとみられる「Realtek SDK」の脆弱性を標的としたアクセス件数の推移（発信元国・地域別 H30.5.1～H30.5.31）

[i] 宛先 IP アドレスと TCP シーケンス番号の初期値が同一である宛先ポート 23TCP 及び 52869TCP に対するアクセス

## ３ 対策

家庭用ルータや IoT 機器の利用者は、以下の対策を参考に、総合的にセキュリティ対策を行うことを推奨します。

- 製造元のウェブサイト等で周知される脆弱性情報に注意を払い、脆弱性が存在する場合にはファームウェアのアップデートや、必要な設定変更等の適切な対策を速やかに実施してください。
- 製品によっては、ファームウェアの自動アップデート機能が存在するものもあります。このような製品を使用している場合には、同機能を有効にしてください。
- IoT 機器をインターネットに接続する場合には、直接インターネットに接続せずに、ルータ等を使用してください。
- インターネットからのアクセスを許可する場合は、必要なポートのみに限定してください。また、必要な発信元 IP アドレスのみにアクセスを許可したり、VPN[i] を用いて接続することも検討してください。
- 必要がない限りは、ルータの UPnP[ii] 機能を無効にしてください。
- 初期設定のユーザ名及びパスワードのままでは使用せず、必ず変更してください。また、変更する際は、ユーザ名及びパスワードを推測されにくいものにしてください。
- 製造終了から年月が経過した製品は、製造元が脆弱性への対応を実施しない場合があります。脆弱性が存在するにも関わらず、製造元が対応しない製品は、対応製品への更新を推奨します。

[i] Virtual Private Network の略であり、パケットをカプセル化して通信を行うことにより、インターネットその他の公衆回線をあたかも専用線であるかのように利用できるサービス。また、カプセル化だけでは、内容の盗聴、改ざんの可能性があるため通信内容を暗号化している場合が多い。

[ii] Universal Plug and Play の略であり、コンピュータ、周辺機器、ネットワーク機器等を相互に自動認識させるための機能。ネットワーク内の機器の検出や機能・サービスを利用するための設定を、複雑な操作をすることなくネットワークに接続するだけで自動的に行うことが可能となります。