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

平成 30 年6月 13 日

Topic

宛先ポート 80/TCP に対する Mirai ボットの特徴を有するアクセスの増加について

宛先ポート 80/TCP に対する Mirai ボットの特徴を有するアクセスの増加を観測しました。ネットワークビデオレコーダ等の IoT 機器をインターネットに接続する場合は、適切なアクセス制限等の対策を早急に実施することを推奨します。

1 宛先ポート 80/TCP に対する Mirai ボットの特徴を有するアクセスの増加の観測

平成 30 年6月 10 日以降、警察庁のインターネット定点観測システムにおいて、宛先ポート 80/TCP に対する Mirai ボットの特徴を有するアクセスの増加を観測しました(図1)。

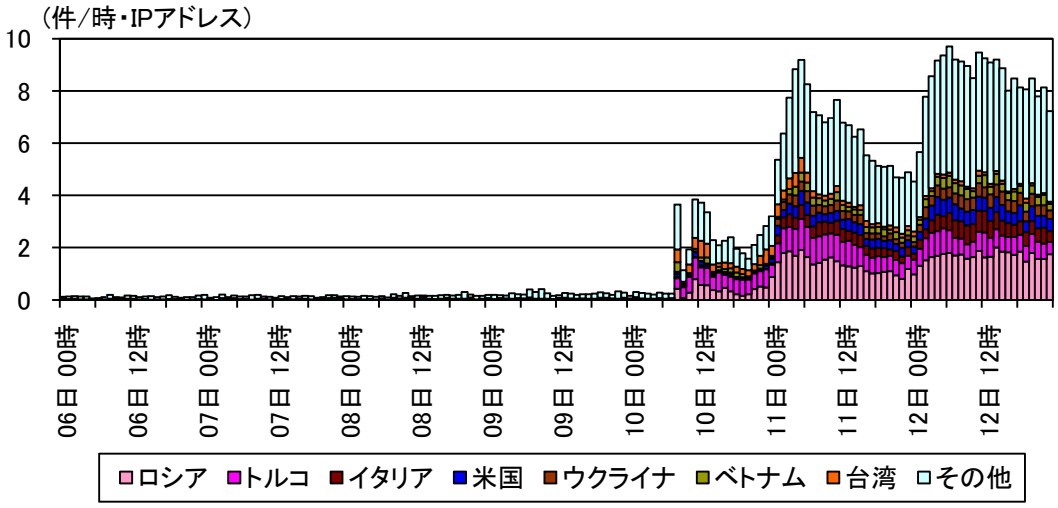

図1 宛先ポート 80/TCP に対する Mirai ボットの特徴を有するアクセス件数の国別推移
(H30.6.6～6.12)

観測したアクセスは、宛先 IP アドレスと TCP シーケンス番号[i]の初期値が一致する Mirai ボットの特徴を有しています。また、HTTP GET リクエストを送信していることから、Web サーバの稼働確認やサーバソフトウェアの種別判定を行っているものと見られます。

また、当該アクセスの発信元について調査したところ、その多くでネットワークビデオレコーダ等のさまざまな IoT 機器に搭載されている Web サーバソフトウェア XiongMai uc-httpd (以下、「uc-httpd」という。)が稼働していることを確認できました。

uc-httpd については、平成 29 年5月にディレクトリトラバーサルの脆弱性(CVE-2017-7577[ii] 及び JVNDB-2017-002986[iii])が公開され、6月8日にもバッファオーバーフローの脆弱性

[i] TCP パケットの送受信状況を管理するための番号で、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、進行に合わせて増加します。また、この初期値を特に ISN(Initial Sequence Number)といいます。
[ii] 「CVE-2017-7577 Detail」
https://nvd.nist.gov/vuln/detail/CVE-2017-7577
[iii] XiongMai uc-httpd におけるディレクトリトラバーサルの脆弱性
https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-002986.html

（CVE-2018-10088 [i] ）が公開されています。

今回の観測は、これらの脆弱性に関連する、IoT 機器に感染した Mirai ボットの亜種による探索活動と考えられます。

日本国内からの宛先ポート 80/TCP に対する Mirai ボットの特徴を有するアクセスも6月 11 日から急増しており、国内においてもこれらの影響を受けている IoT 機器が存在していると考えられます（図2）。

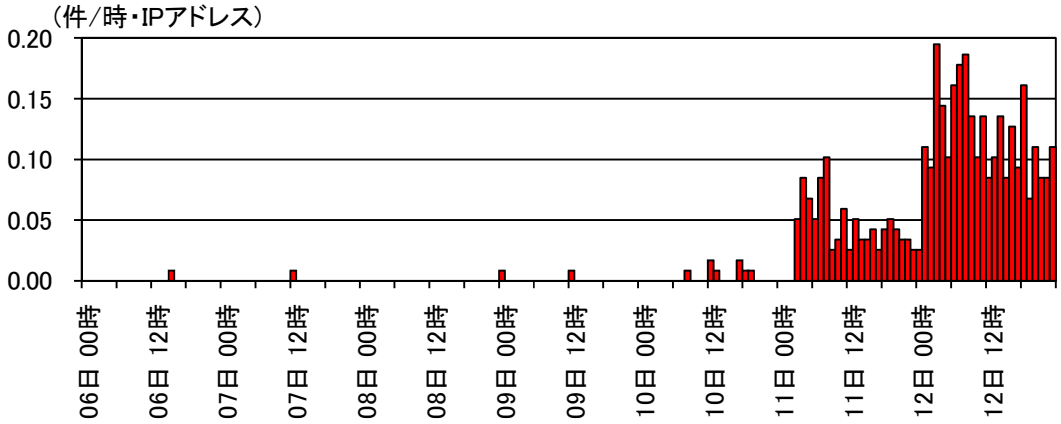

図2　宛先ポート 80/TCP に対する Mirai ボットの特徴を有する国内からのアクセス件数の推移（H30.6.6～6.12）

2　推奨する対策

今回の観測との関連の有無にかかわらず、ネットワークビデオレコーダ等の 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。

- 該当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するのではなく、ルータ等を使用してください。また、ファイアウォール等によって不必要な外部からのアクセスを遮断する、特定の IP アドレスのみにアクセスを許可する等の適切なアクセス制限を実施してください。
- ユーザ名及びパスワードは、初期設定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かかわらず、製造元が対応しない製品は、使用を中止してください。
- 製造元のウェブサイト等で脆弱性情報を確認し、脆弱性がある場合はファームウェアのアップデート等の適切な対策を実施してください。

[i] 「CVE-2018-10088 Detail」
https://nvd.nist.gov/vuln/detail/CVE-2018-10088