レポート

平成 30 年 7月 23 日

宛先ポート 80/TCP、8000/TCP、8888/TCP 等に対するアクセスの増加について

- 宛先ポート 80/TCP 及び 8000/TCP に対する Mirai ボットの特徴を有するアクセスの増加
- 宛先ポート 8888/TCP 等に対するアクセスの増加

1 宛先ポート 80/TCP 及び 8000/TCP に対する Mirai ボットの特徴を有するアクセスの増加

警察庁のインターネット定点観測システムにおいて、平成 30 年6月 10 日以降、宛先ポート 80/TCP に対するアクセスの増加を観測しました。このアクセスは、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おり、平成 30 年6月 13 日に注意喚起 [ii] を実施しています。アクセス件数は、6月 15 日以降に一旦減少しましたが、6 月 22 日再び増加する等の推移がありました（図1）。

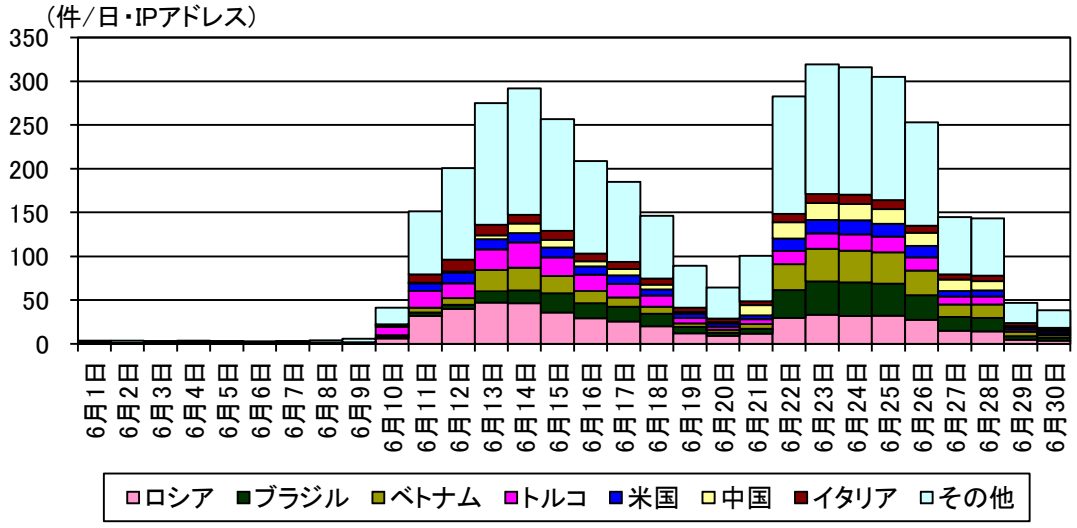

図1 宛先ポート 80/TCP に対する Mirai ボットの特徴を有するアクセス件数の推移
（発信元国・地域別 [iii] H30.6.1～6.30）

[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] 「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」
https://www.npa.go.jp/cyberpolice/important/2018/201806131.html

[iii] 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。

また、6月 14 日以降、宛先ポート 8000/TCP に対する Mirai ボットの特徴を有するアクセスの増加も観測しました（図2）。

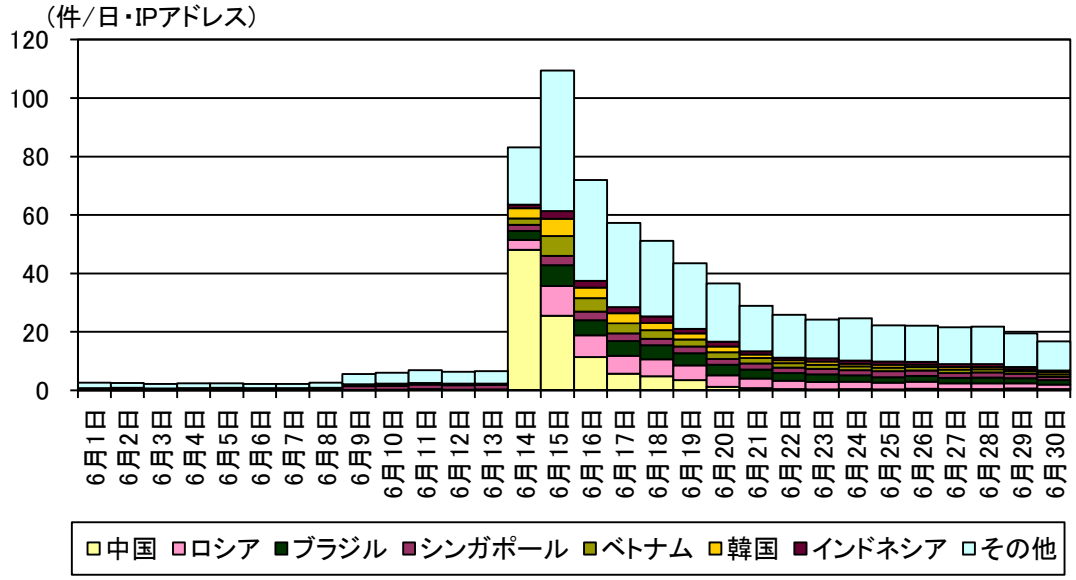

図2　宛先ポート 8000/TCP に対する Mirai ボットの特徴を有するアクセス件数の推移
（発信元国・地域別　H30.6.1～6.30）

観測したアクセスは、HTTP GET リクエストを送信していることから、Web サーバの稼動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様々な 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。）が稼動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 [i] 及び JVNDB-2017-002986 [ii] ）が公開され、本年6月８日にもバッファオーバーフローの脆弱性（CVE-2018-10088 [iii] ）が公開されています。

宛先ポート 8000/TCP に対するアクセスは、宛先ポート 80/TCP に対するアクセスと同様に、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。

[i] 「CVE-2017-7577 Detail」
https://nvd.nist.gov/vuln/detail/CVE-2017-7577
[ii] 「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
[iii] 「CVE-2018-10088 Detail」
https://nvd.nist.gov/vuln/detail/CVE-2018-10088

日本国内からの宛先ポート 80/TCP 及び 8000/TCP に対する Mirai ボットの特徴を有するアクセスも観測しており（図3）、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るため、引き続き注意が必要です。

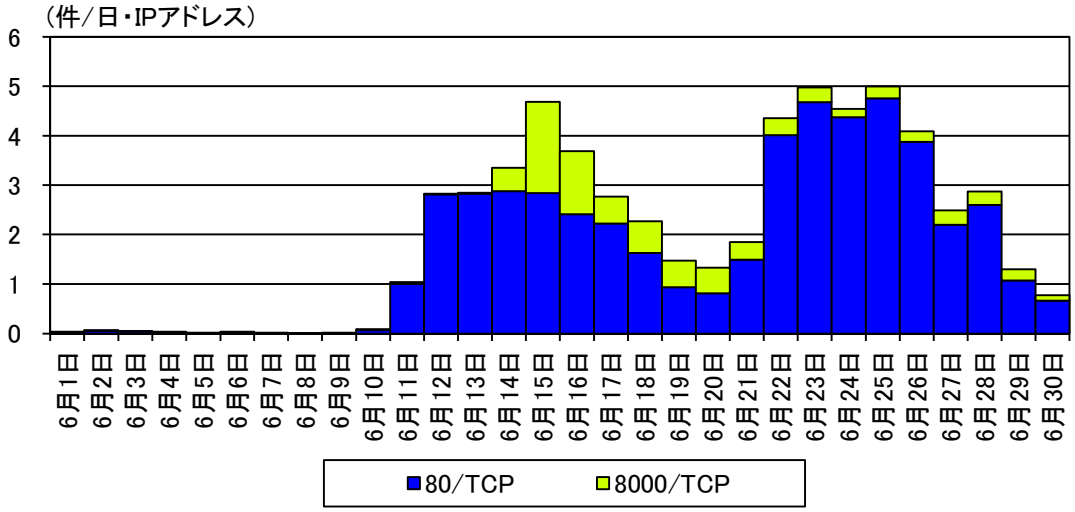

図3　宛先ポート 80/TCP 及び 8000/TCP に対する Mirai ボットの特徴を有する国内からのアクセス件数の推移（宛先ポート別　H30.6.1～6.30）

2　宛先ポート 8888/TCP 等に対するアクセスの増加

平成 30 年5月 30 日以降、宛先ポート 8888/TCP 等に対するアクセスの増加を観測しました（図4）。

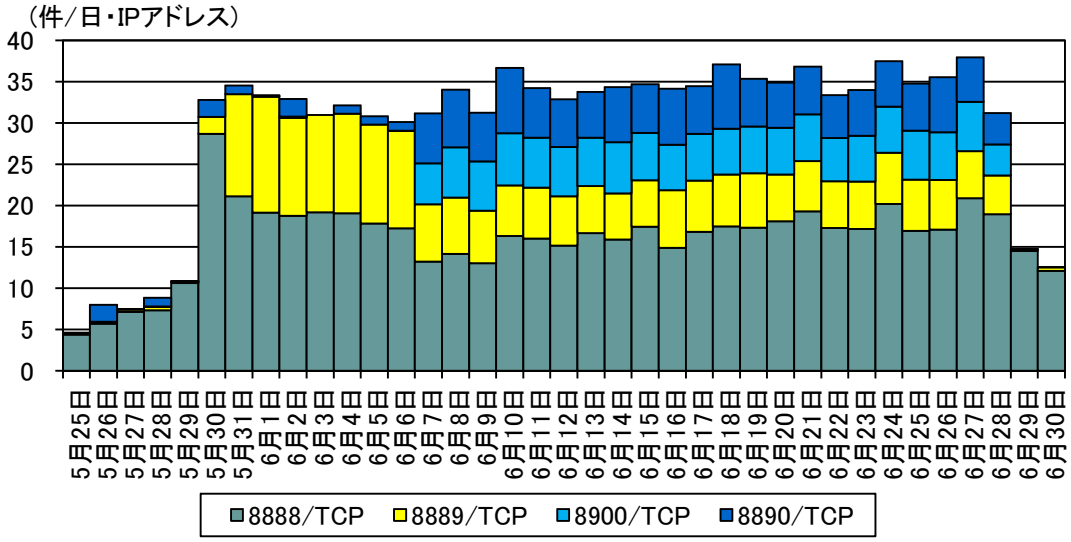

図4　宛先ポート 8888/TCP 等に対するアクセス件数の推移（宛先ポート別　H30.5.25～6.30）

これらのうち、宛先ポート 8888/TCP に対するアクセスには、宛先 IP アドレスと TCP シーケンス番号の初期値が一致する Mirai ボットの特徴を有するアクセスが含まれており、発信元 IP アドレスを調査したところ、前項で観測した Mirai ボットの特徴を有するアクセスの発信元と同一のものが多数含まれていました。

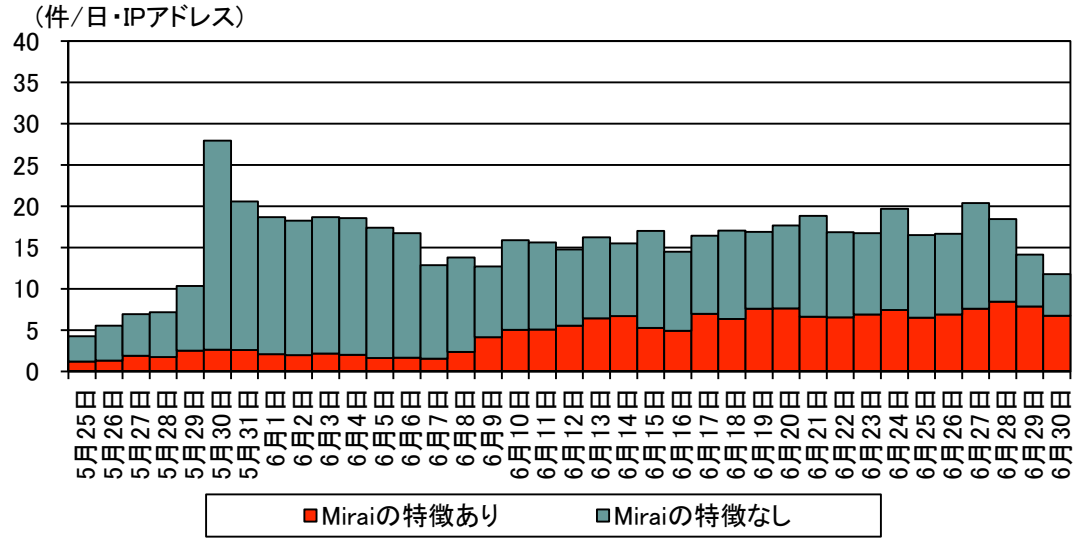

図5　宛先ポート 8888/TCP に対するアクセス件数の推移（Mirai ボットの特徴有無別　H30.5.25～6.30）

また、平成 30 年5月 24 日には、仮想通貨「EOS（イオス）」において「RPC API」を使用して秘密鍵が表示される問題があることが海外の開発プラットフォームにおいて公表[i]されました。この「RPC API」が悪用された場合、HTTP リクエストに特定の文字列を挿入することで秘密鍵を取得することが可能であるとされています。

今回観測した宛先ポート 8888/TCP 等に対するアクセスの中に、Mirai ボットの特徴を有するアクセスとは異なり、当該「RPC API」を使用した仮想通貨「EOS」を標的としたアクセスも含まれていることを確認しました（図6）。

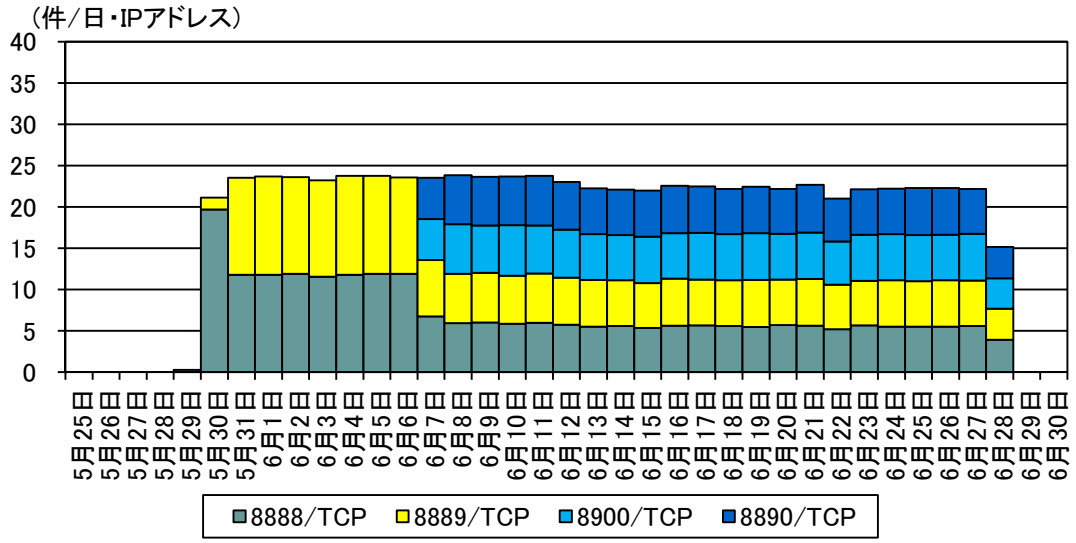

図6　仮想通貨「EOS」を標的としたアクセス件数の推移（宛先ポート別　H30.5.25～6.30）

観測したアクセスは、秘密鍵を取得する「RPC API」を使用し、情報の取得を試みるものでした（図7）。

```
GET [redacted]list_keys HTTP/1.1
Host: [redacted]:8888
```

図7　秘密鍵を取得する「RPC API」を使用した観測したアクセスの例（一部をマスキング）

さらに、警察庁の定点観測システムにおいて、5月 27 日と6月4日に、仮想通貨「EOS」に関するノードの最新情報を取得する「RPC API」を使用した 8888/TCP へのアクセスも観測しました（図8及び図9）。

[i] https://github.com/EOSIO/eos/issues/3372

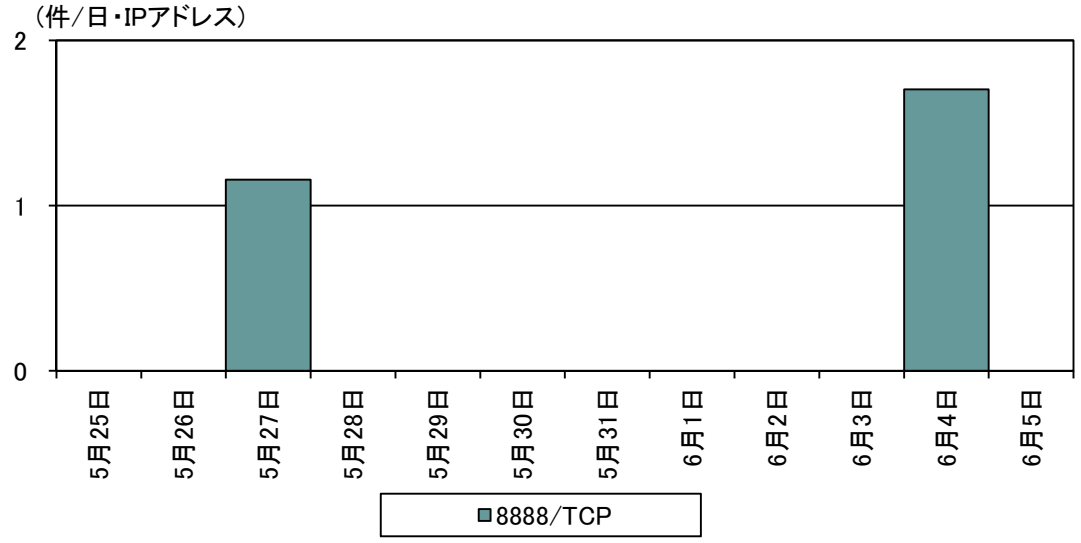

図8　ノードの最新情報を取得する「RPC API」を使用したアクセス件数の推移（H30.5.25～6.5）

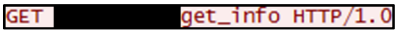

図9　ノードの最新情報を取得する「RPC API」を使用したアクセスの例（一部をマスキング）

このようなことから、今回の観測は、IoT 機器に感染した Mirai ボットの亜種による探索活動及び仮想通貨「EOS」を標的とした秘密鍵やノード情報の探索活動を観測したものと考えられます。

３ 対策

サーバ等及び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。

- IoT 機器やサーバ等をインターネットに接続する場合は、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。
- 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。
- 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。
- 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。