レポート

平成 31年2月1日

32764/TCP 及び 37215/TCP に対する Mirai ボットの特徴を有するアクセスの増加等について

- 32764/TCP 及び 37215/TCP に対する Mirai ボットの特徴を有するアクセスの増加
- リモートデスクトップサービスを標的としたアクセスの増加

1 32764/TCP 及び 37215/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において、平成 30 年 11 月中旬以降、宛先ポート 32764/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という Mirai ボットの特徴を有していました。(図1)。

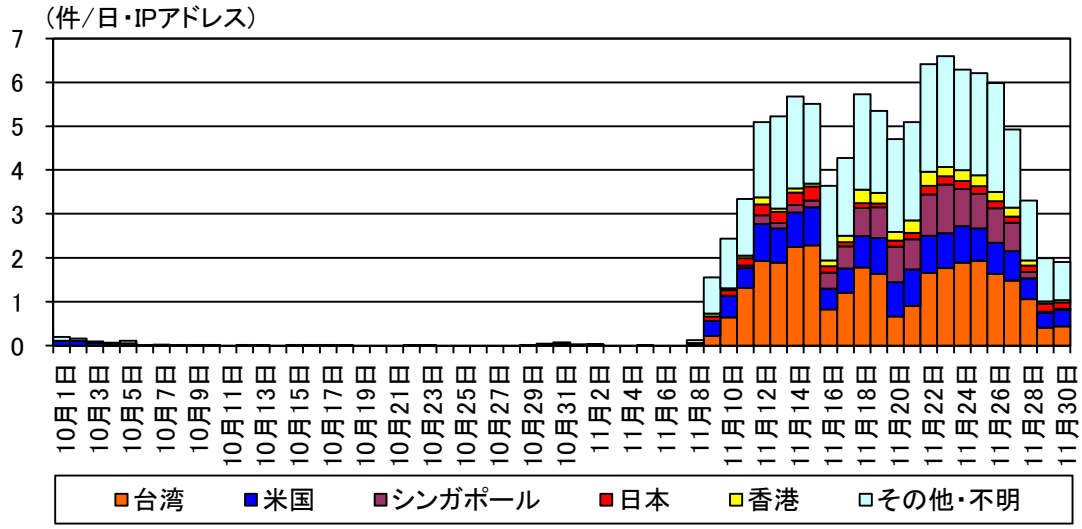

図1 宛先ポート 32764/TCP に対する Mirai ボットの特徴を有するアクセス件数の発信元国・地域別[ii] 推移(H30.10.1～11.30)

ポート 32764/TCP は、過去の Cisco 社製ルータ等においてテストインタフェースとして使用されていました。当該ルータについては、平成 26 年に脆弱性が公表[iii]されており、第三者によりテストインタフェースへのリクエストを介して、資格情報及び構成データを読み取られ、任意のコ

[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] 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。

[iii] JVNDB-2014-001039
複数の Cisco 製品のファームウェアにおける資格情報および構成データを読まれる脆弱性
https://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-001039.html

マンドを実行される可能性があります。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、ウェブサーバの稼動確認等を行っているものと推測されます。

同アクセスの発信元 IP アドレスを調査したところ、海外製ルータ、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、同年 12 月以降は、宛先ポート 37215/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、その中には国内を発信元とするアクセスも多くありました（図2）。

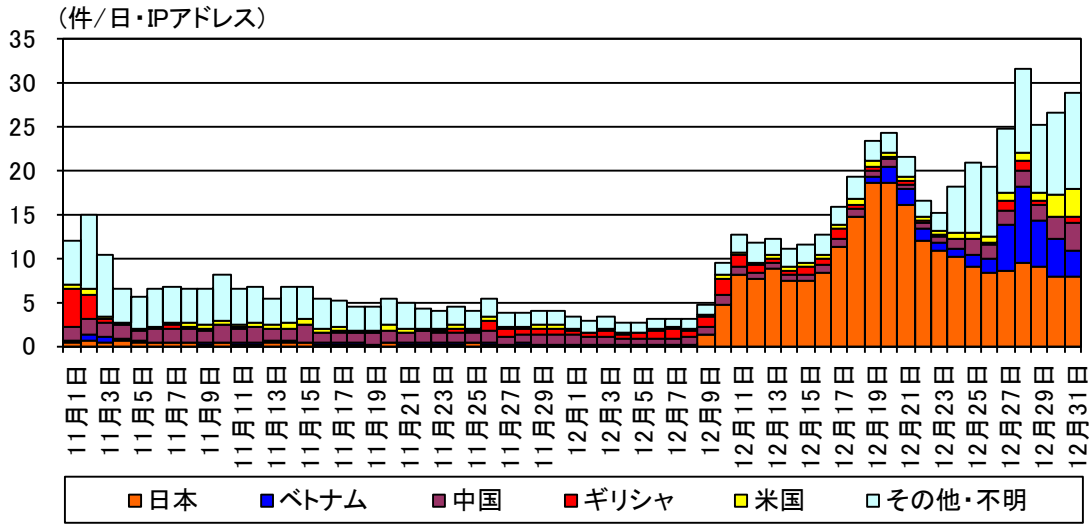

図2　宛先ポート 37215/TCP に対する Mirai ボットの特徴を有するアクセス件数の発信元国・地域別[i]推移（H30.11.1～12.31）

宛先ポート 37215/TCP は、既に平成 29 年 11 月末に公開されている、Huawei 製ルータに関する、リモートからの任意のコード実行が可能となる脆弱性（CVE-2017-17215 [ii] ）に関連しているものです。今回観測したアクセスには、本脆弱性を標的としたものが多数存在することを確認しています（図3）

図3　観測したアクセスの例（一部マスキング）

[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。

[ii] 「CVE-2017-17215 Detail」
https://nvd.nist.gov/vuln/detail/CVE-2017-17215

これらのアクセスは、感染したMiraiボットの亜種が既知の脆弱性を対象に探索活動を行ったものと考えられます。

また、国内を発信元とするアクセスも多く観測していることから、国内でもMiraiボットの亜種に感染した機器が多く存在していると考えられます。

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機能を無効にしてください。
- ユーザ名及びパスワードは、初期設定のままで使用せず、必ず変更してください。また、ユーザ名及びパスワードを変更する際は、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、製造元のサポートが終了し、脆弱性への対応が実施されない場合があります。そのような製品を使っている場合には、サポート中の製品への更新を推奨します。

２ リモートデスクトップサービスを標的としたアクセスの増加

警察庁のインターネット定点観測において、平成 30 年 11 月下旬頃からリモートデスクトップサービスを標的とした宛先ポート 3389/TCP に対するアクセスの増加を観測しました（図4、図5）。

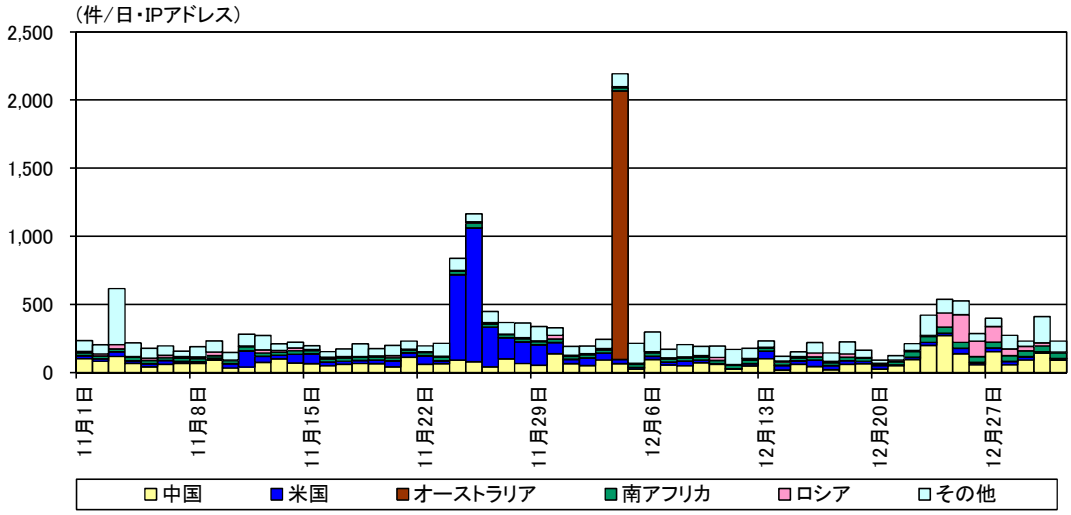

図4　リモートデスクトップサービスを標的とした宛先ポート 3389/TCP に対するアクセス件数の発信元国・地域別推移（H30.11.1～12.31）

図5　観測したアクセスの例（一部抜粋、マスキングを実施）

リモートデスクトップサービスとは、Microsoft Windows の遠隔操作に使用されるサービスで、主にポート 3389/TCP を使用します。

同アクセスのほとんどは IP ヘッダの TTL 値が 64 以上 128 未満となっていることから、発信元となっている機器の多くは Microsoft Windows が動作していると推測されます。また、発信元の機器には、リモートデスクトップサービスにアクセス可能なものが多数ありました（図6）。

図6　発信元機器のリモートデスクトップサービスに対するアクセスの例
（一部抜粋、マスキングを実施）

なお、今回のアクセスとの直接の関係は不明ですが、平成 30 年 12 月3日に US-CERT からランサムウェア「SamSam」について注意喚起[i]がされています。「SamSam」は、ファイルを暗号化し、復号を条件に金銭を要求するランサムウェアです。当該ランサムウェアは、平成 27 年 12 月に作成され、平成 29 年6月及び 10 月には巧妙化した亜種が確認されています。当該ランサムウェアの感染状況[ii]は、米国が中心ですが、同国以外にもカナダ、英国、中東諸国等において攻撃が確認されています。また、リモートデスクトップサービスへのブルートフォース攻撃[iii]を実施する機能を有していることから、これにより宛先ポート 3389/TCP 宛のアクセスが増加した可能性が考えられます。

リモートデスクトップサービスの利用者は、以下の対策を参考にセキュリティ対策を行うことを推奨します。

- リモートデスクトップサービスを用いてインターネット経由で接続する場合には、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。
- リモートからアクセス可能なユーザを必要最小限に限定してください。
- ユーザ名及びパスワードは推測されにくいものにしてください。
- 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。

---

[i] Alert (AA18-337A) SamSam Ransomware
https://www.us-cert.gov/ncas/alerts/AA18-337A

[ii] SamSam: 600 万ドル近くの身代金を手にしたランサムウェア
https://www.sophos.com/ja-jp/medialibrary/PDFs/technical-papers/SamSam-The-Almost-Six-Million-Dollar-Ransomware.pdf

[iii] 総当たり攻撃ともいう。可能な組み合わせを全て試す手法。