JPCERT CC®

Japan Computer Emergency Response Team Coordination Center

JPCERT-TBM-2018-01
発行日：2018-4-26

JPCERT/CC インターネット定点観測レポート
[2018 年 1 月 1 日～3 月 31 日]

1. 概況

JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、不特定多数に向けて発信されるパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類して、これを脆弱性情報、マルウエアや攻撃ツールの情報などと対比して分析することで、攻撃活動や準備活動の捕捉に努めています。また、こうした観測では、複数の視点による多元的な見方も重要であるため、主に海外の National CSIRT と連携してそれぞれの組織にセンサーを設置し観測網に参加してもらう活動を行っています。各地のセンサーから収集したデータを分析し、問題が見つかれば、適切な地域の National CSIRT 等に情報を提供し、状況の改善を依頼しています。また、日本国内固有の問題については、JPCERT/CC の日々の活動の中で対処しています。
本レポートでは、本四半期に国内に設置されたセンサーで観測されたパケットを中心に分析した結果について述べます。

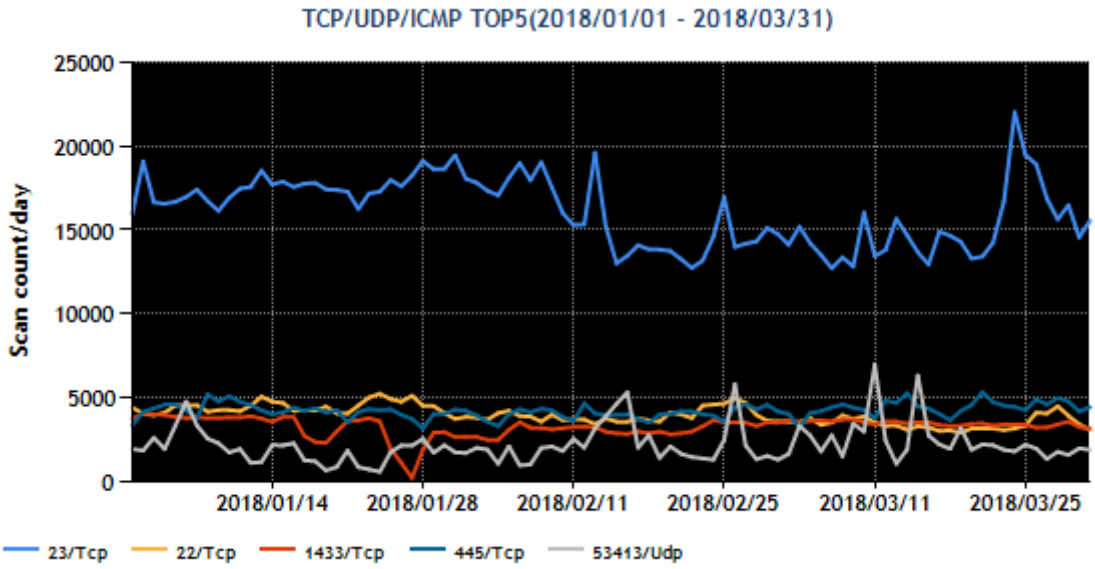
宛先ポート番号別パケット観測数のトップ 5 を［表 1］に示します。

［表 1：宛先ポート番号トップ 5］

順位	宛先ポート番号	前四半期の順位
1	23/TCP (telnet)	1
2	22/TCP (ssh)	2
3	1433/TCP(ms-sql-s)	4
4	445/TCP(microsoft-ds)	3
5	53413/UDP	6

※ポート番号とサービスの対応の詳細は、IANA の文書(*1)を参照してください。なお、サービス名は IANA の情報をもとに記載していますが、必ずしも各サービスプロトコルに則ったパケットが受信されているとは限りません。

図 1 は、期間中のトップ 5 の宛先ポート番号ごとのパケット観測数の推移を示しています。



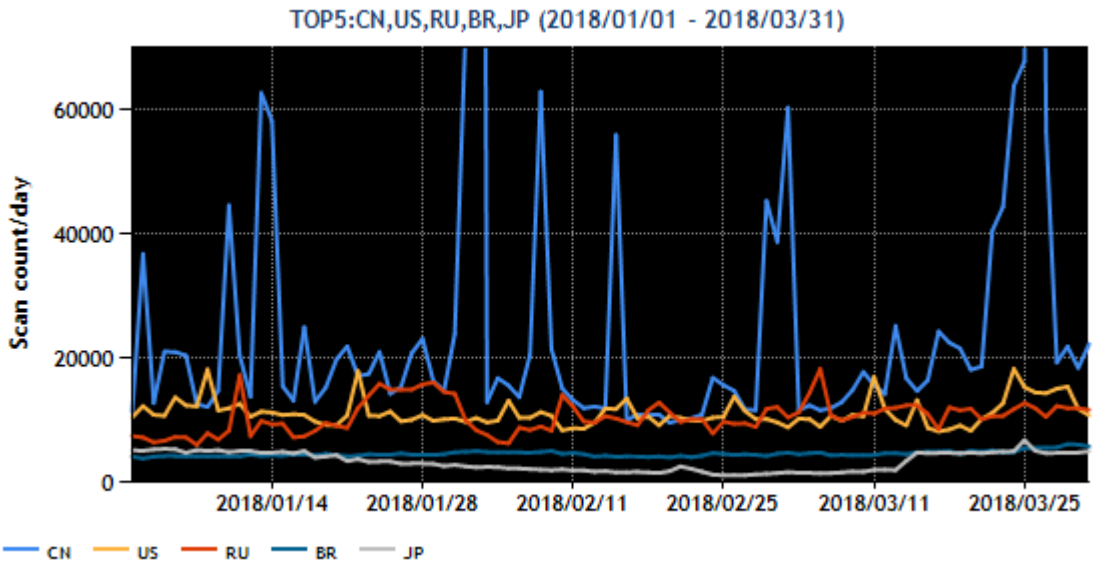
［図 1：2018 年 1～3 月の宛先ポート番号別パケット観測数トップ 5 の推移］

送信元地域のトップ 5 を［表 2］に示します。

［表 2：送信元地域トップ 5］

順位	送信元地域	前四半期の順位
1	中国	1
2	米国	2
3	ロシア	3
4	ブラジル	4
5	日本	5

図 2 に期間中のトップ 5 のパケット送信元地域からのパケット観測数の推移を示します。



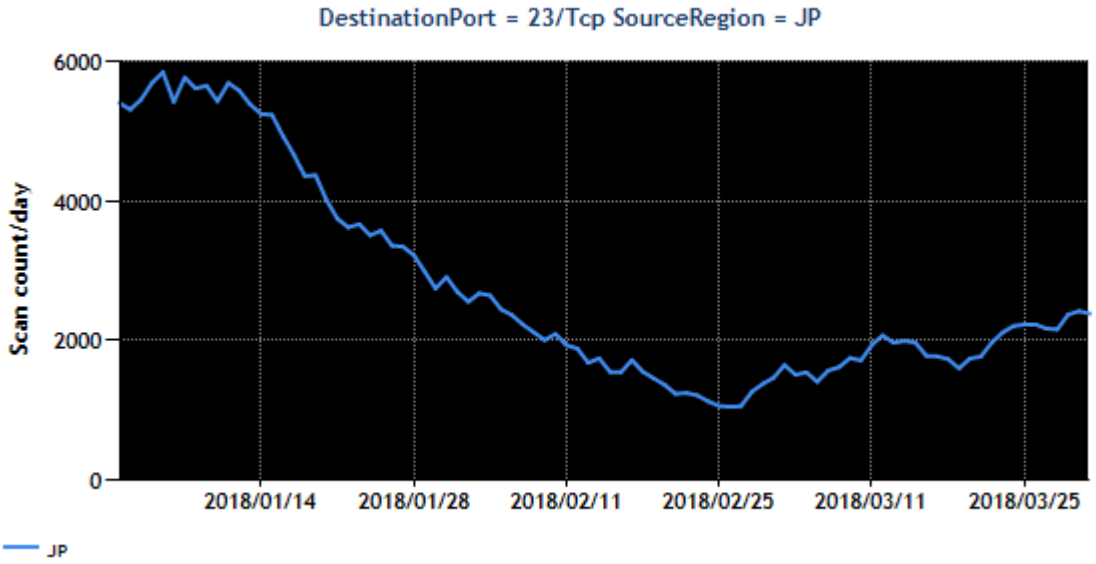
［図 2：2018 年 1～3 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

前四半期同様に本四半期も、Windows の SQL Server と SMB サービスのリクエストパケットが多数観測されました。また、SSH（22/TCP）や Telnet（23/TCP）のリクエストパケットも前四半期に続きトップ 5 に入る数を観測しており、脆弱な Web カメラ、ルータ、NAS 等の機器の探索が継続して行われているものと推測されます。また、日本国内で販売されていたある無線 LAN ルータの脆弱性が悪用されることで Mirai 亜種に感染し、さらに感染を広げるためのパケットを送信しているという先四半期の報告(*2)で述べた状況は今四半期も継続して観測されています。その他に関しては、特筆すべき状況の変化は見られませんでした。

2. 注目された現象

2.1. 日本国内の IP アドレスからの 23/TCP 宛のパケットの観測状況について

送信元 IP アドレスが日本国内で 23/TCP 宛のパケット観測数の 1 月から 3 月にかけての推移を図 3 に示します。これらのパケットの送信元のほとんどは Mirai の亜種に感染した機器であると推測されます。



［図 3：Port23/TCP 宛のパケットの観測数の推移］

Mirai の背後にいる攻撃者は、攻撃対象や手法を時に応じて変えており、それに合わせるように異なる亜種を繰り出しているようです。Mirai やその亜種に感染した機器は、感染時に使用した攻撃手法への一時的な対策を行うことで別の亜種への感染を防ぐ場合もあります。しかし、抜本的な対策が行われていない機器では、マルウエアにより再起動される、またはユーザが自ら機器の再起動を行うことを契機として感染状態を脱し、再び新たな Mirai 亜種に感染することがあります。そのため、インターネット全体としては、Mirai 亜種に感染している機器の内訳が徐々に変化しています。
23/TCP 宛のパケットの観測数の増減は、Mirai の亜種それぞれが対象とする感染機器の台数の推移にブレークダウンすることができます。すなわち、図 3 に示したような、日本国内から送信された 23/TCP 宛のパケット観測数の 2 月末にかけての現象とそれ以降の増加から次のことが推測されます。

- 2 月のある時期までは、攻撃者は日本国内で販売されていたある無線 LAN ルータを対象に Mirai の亜種に感染させようとしていたが、機器ベンダー(*3)や ISP、セキュリティ機関等(*4)の対策の呼びかけによってユーザによる対策が進んだことにより、感染した機器の台数が減少していった。

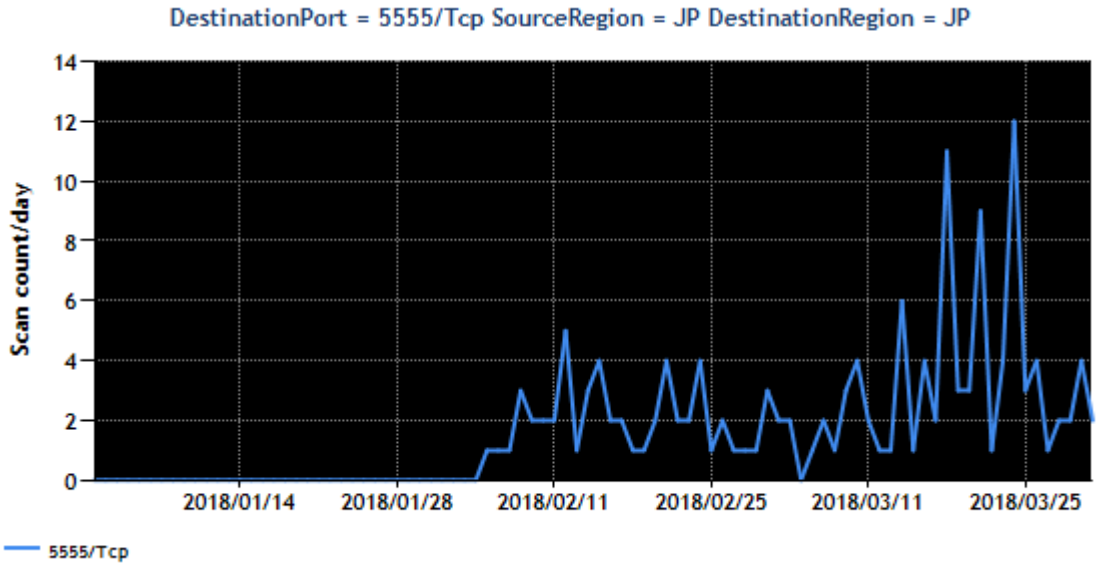
- 2 月末になって、攻撃者が日本国内で販売されていた前項と同じ機種のルータを対象とした Mirai の亜種を用いた攻撃を再開したことに伴って、再起動により感染状態から脱していた機器が再び感染し、一時的にパケットを観測しなくなった IP アドレスからのパケットが再度送信され始めた。

この推測を裏付けるように、2 月 26 日以降に再度パケットを観測した 23/TCP 宛のパケットの送信元

IP アドレスの管理者に情報を提供したところ、2017 年 12 月 19 日に公表した注意喚起に記載されている製品を使用していたとの回答が複数ありました。
対策されていない機器がまだ使用されているとみられるため、注意喚起情報(*5)の「対象」に列挙されたルータを使用してインターネットに接続している場合は、対策を実施してください。

2.2. 5555/TCP 宛のパケット数の観測状況について

2018 年 2 月 4 日頃より、Port5555/TCP 宛のパケットを観測しています。送信元には国内外の IP アドレスのパケットがありますが、図 4 に国内の IP アドレスのパケット数の推移を示します。



［図 4. Port5555/TCP 観測パケット数の主な送信元地域ごとの内訳の推移］

これらのパケットは、Mirai に感染した端末からのパケットと共通した特徴を有していることから、Mirai の亜種に感染した端末によるものと推測されます。パケットは 5555/TCP を宛先としており、ほかのポート番号へのパケットはほとんど観測されていません。
また、感染した端末の機種を特定するため、日本国内の一部の送信元にアクセスしてみましたが、5555/TCP が開いていることが確認できただけで、機種を特定できるような情報は得られませんでした。送信元 IP アドレスの管理者へ照会したところ、一部の方から海外製のインターネット TV チューナー機器（以下「TV box」）を、ルータやファイアウォールなどを介さずにインターネットに接続していたとの回答がありました。
当該 TV box の製品仕様を確認したところ、Android OS を使用していることがわかりました。今回、パケットの宛先ポート番号となった 5555/TCP は、Android OS にはネットワークを介してデバッグ用の adb コマンドを受け付ける機器上のデーモン(*6)が使用する一部のポート番号で、開発完了後は必要ないため閉じておくべきものです。攻撃者は遠隔より接続が可能なネットワーク経由でのデバッグが可能な機器の探索や攻撃を行っていた可能性が高いと考えられます。同時期に海外では仮想通貨の一種「Monero」のマイニングの試行を行うマルウエアが「Mirai」のコードを流用し、同ポートへの通信を試みる活動を行っていたとの調査結果(*7)があり、日本国内でもデバッグ用の adb コマンドを受け付ける機

器が設置され、本攻撃活動の影響を受けたと考えられます。それ以外にも同様の問題をもつ機器がある可能性があるため継続して情報収集を行っています。
ネットワークに接続する機器は、攻撃を受ける可能性があるため、ファイアウォール等で適切なアクセス制御を行い、不審な通信が発生していないか確認することをおすすめします。

3. 参考文献

(1) Service Name and Transport Protocol Port Number Registry
https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

(2) インターネット定点観測レポート(2017 年 10～12 月)
https://www.jpcert.or.jp/tsubame/report/report201710-12.html

(3) ロジテック製 300Mbps 無線 LAN ブロードバンドルータおよびセットモデル (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

(4) ルータ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
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
https://www.npa.go.jp/cyberpolice/important/2017/201712191.html
Mirai 亜種の感染拡大に伴う注意喚起
https://wizsafe.iij.ad.jp/2017/12/175/

(5) 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

(6) Android Debug Bridge
https://developer.android.com/studio/command-line/adb.html?hl=ja

(7) ADB.Miner: More Information
http://blog.netlab.360.com/adb-miner-more-information-en/

本活動は、経済産業省より委託を受け、「平成 29 年度サイバー攻撃等国際連携対応調整事業」として実施したものです。