JPCERT CC®

JPCERT-TBM-2018-03
発行日：2018-08-02

JPCERT/CC インターネット定点観測レポート
[2018 年 4 月 1 日～6 月 30 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。

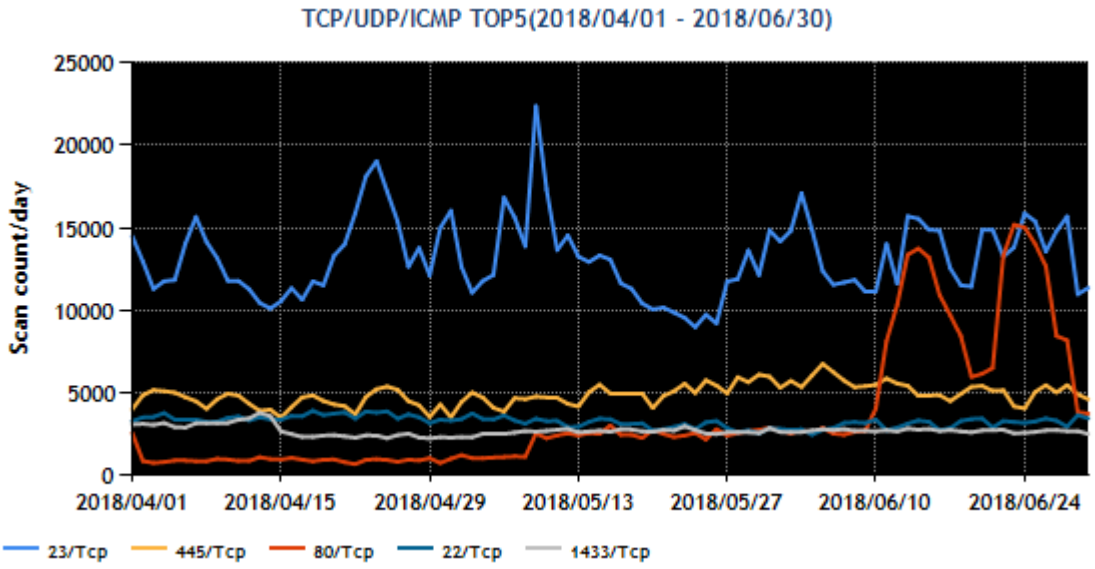
宛先ポート番号別パケット観測数のトップ 5 を［表 1］に示します。

［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	445/TCP(microsoft-ds)	4
3	80/TCP(http)	TOP10 外
4	22/TCP (ssh)	3
5	1433/TCP(ms-sql-s)	2

※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、本四半期中のトップ 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。



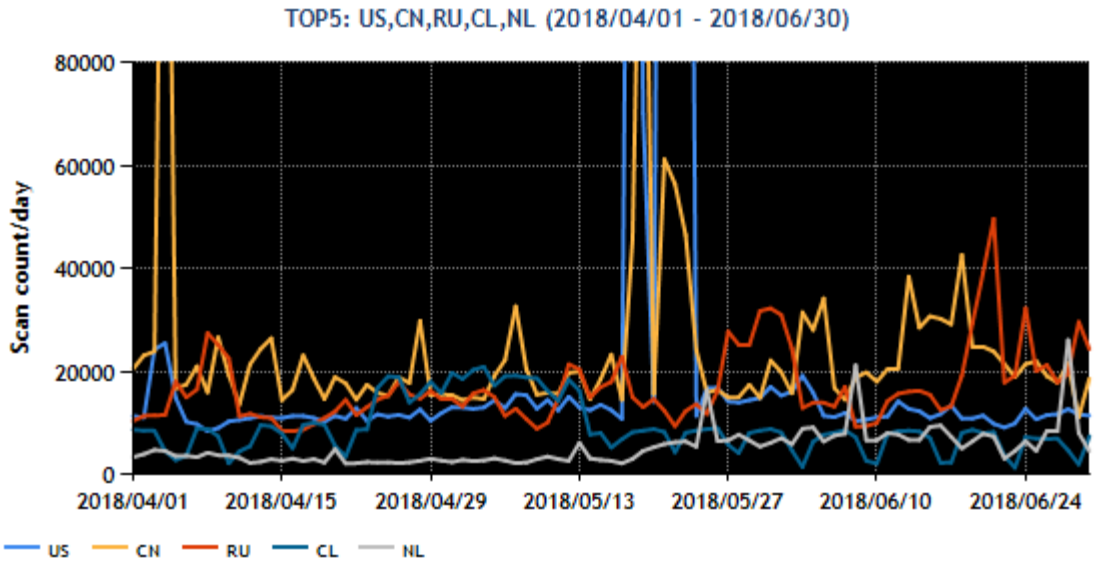
［図 1：2018 年 4～6 月の宛先ポート番号別パケット観測数トップ 5 の推移］

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	米国	2
2	中国	1
3	ロシア	3
4	チリ	TOP10 外
5	オランダ	7

［図 2］に本四半期中のトップ 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。



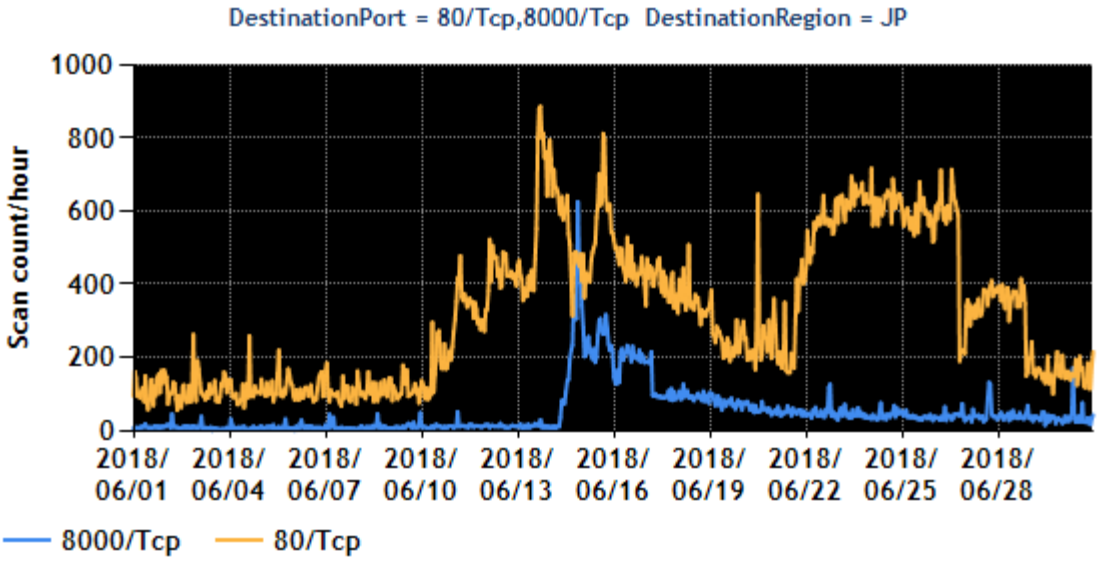
［図 2：2018 年 4～6 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

本四半期は、6 月の中旬から 80/TCP 宛を対象とするパケットが増加しています。この件については、後の 2.1 注目された現象で取り上げます。そのほか、前四半期同様 Windows の SQLServer と SMB サービスのリクエスト受付用ポートに対するパケットを観測しました。その他、前四半期もトップ 5 に入っていた、脆弱な Web カメラ、ルータ、NAS 等の機器を狙ったとみられる 22/TCP や 23/TCP 等の宛先ポートに対するパケットも継続して観測されました。送信元地域の順位が変化したのは、オランダからは UDP リフレクション攻撃の踏み台を探索するパケットを、チリからは分散型アプリケーション用プラットフォームが使用するポートを探索するパケットを継続的に観測したためです。

2. 注目された現象

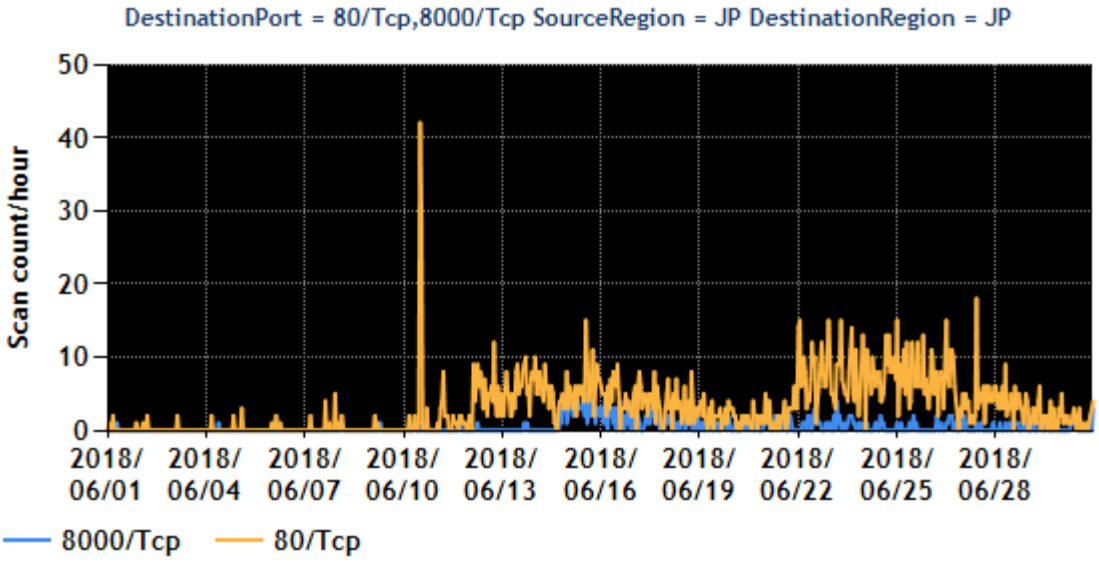
2.1. Port80/TCP、Port8000/TCP 宛のパケット数の増加

6 月 10 日から、Port80/TCP(*2*3*4*5)に対するパケットを継続して観測しました。14 日(*6)からは Port8000/TCP に対するパケットを観測しました。［図 3］



［図 3：Port80/TCP、Port8000/TCP 宛のパケットの観測数の推移］

送信先 IP アドレスと TCP ヘッダのシーケンス番号が一致しており、これはマルウエア Mirai が送信するパケットの特徴です。送信元地域はさまざまですが、日本国内から送信されたパケットも確認しています。［図 4］



［図 4：Port80/TCP、Port8000/TCP 宛のパケットで日本から送信されたパケットの観測数の推移］

これらのパケットの送信元になっている日本国内の IP アドレスの一部にアクセスすると、「Server: uc-httpd/1.0.0」の Web サーバのバナーが表示され、Web カメラやレコーダーとみられるログイン画面が表示されました。uc-httpd/1.0.0 は影響する複数の脆弱性の情報が公開されており、一部の脆弱性については検証用のコードもインターネット上で公開されています。6 月 10 日以降に増加したパケットが、検証用コードを使用した攻撃であったかどうかは不明です。その後、一部の機器がインターネット上に公開している Web サーバに対して、当該検証用コードを使用したと推測される攻撃を行っていることをアクセスログで確認しています。

JPCERT/CC では、TSUBAME で観測したパケットの情報を通信事業者に報告し、送信元となっているユーザへの連絡をお願いしています。

インターネットに直接接続された Web カメラやレコーダー等の機器を利用しているユーザは、インターネットから機器へのアクセスを禁止できないかご検討ください。禁止できない場合は、ファイアウォール等でアクセスを必要最小限に制限し、パスワードを初期設定のものから変更してください。

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) 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/detect/pdf/20180613.pdf

(3) 平成 30 年６月期観測資料
https://www.npa.go.jp/cyberpolice/detect/pdf/20180723_toukei.pdf

(4) 80/TCP 宛通信の増加
http://blog.nicter.jp/reports/2018-04/mirai-80/

(5) Botnets never Die, Satori REFUSES to Fade Away
https://blog.netlab.360.com/botnets-never-die-satori-refuses-to-fade-away-en/

(6) Satori IoT Botnet Variant
https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/satori-iot-botnet/

本活動は、経済産業省より委託を受け、「平成 30 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。