JPCERT Coordination Center

JPCERT/CC インターネット定点観測レポート

2021 年 4 月 1 日 ～ 2021 年 6 月 30 日

一般社団法人 JPCERT コーディネーションセンター

2021 年 7 月 26 日

JPCERT CC®

目次

1. 概況

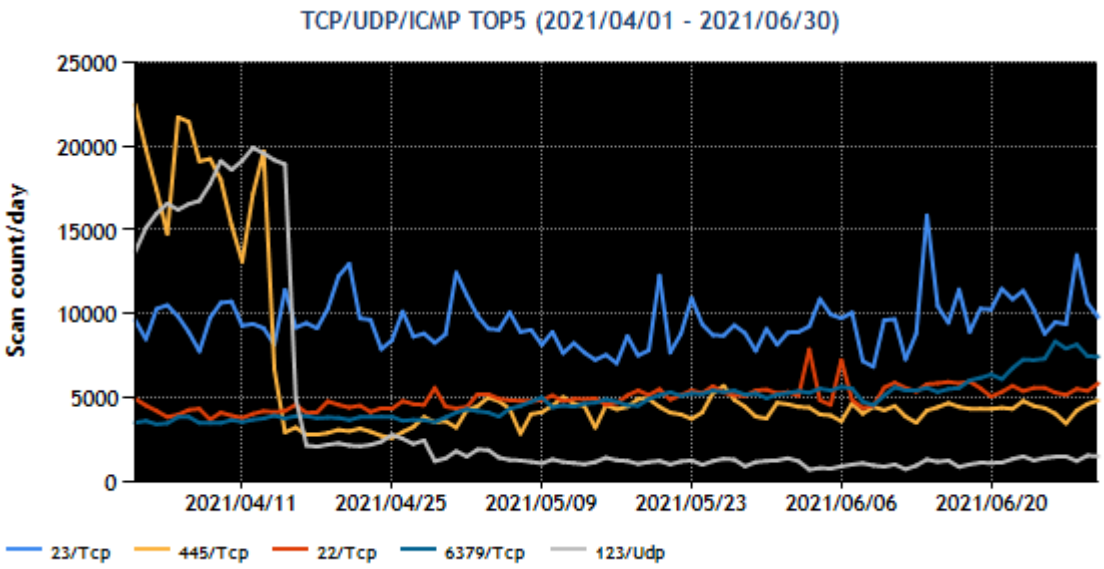
JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、不特定多数に向けて発信されるパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類して、これを脆弱性情報、マルウェアや攻撃ツールの情報などと対比して分析することで、攻撃活動や準備活動の捕捉に努めています。また、こうした観測では、複数の視点からの多元的な見方も重要であるため、主に海外の National CSIRT と連携してそれぞれの組織にセンサーを設置し、観測網に参加してもらう活動を行っています。
各地のセンサーから収集したデータを分析し、問題が見つかれば、適切な地域の National CSIRT などに情報を提供し、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、日本国内に設置されたセンサーで本四半期に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。
本四半期に国内で観測されたパケットの宛先ポート番号をパケットが多かった順に並べた時のトップ 5 は［表 1］に示すとおりでした。

［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	445/TCP (microsoft-ds)	1
2	23/TCP (telnet)	2
3	123/UDP (ntp)	3
4	22/TCP (ssh)	4
5	6379/TCP	10

※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のっとった形式のパケットが受信されているとは限りません。

［表 1］に示した各宛先ポート番号を持つパケット観測数の推移を［図 1］に示します。



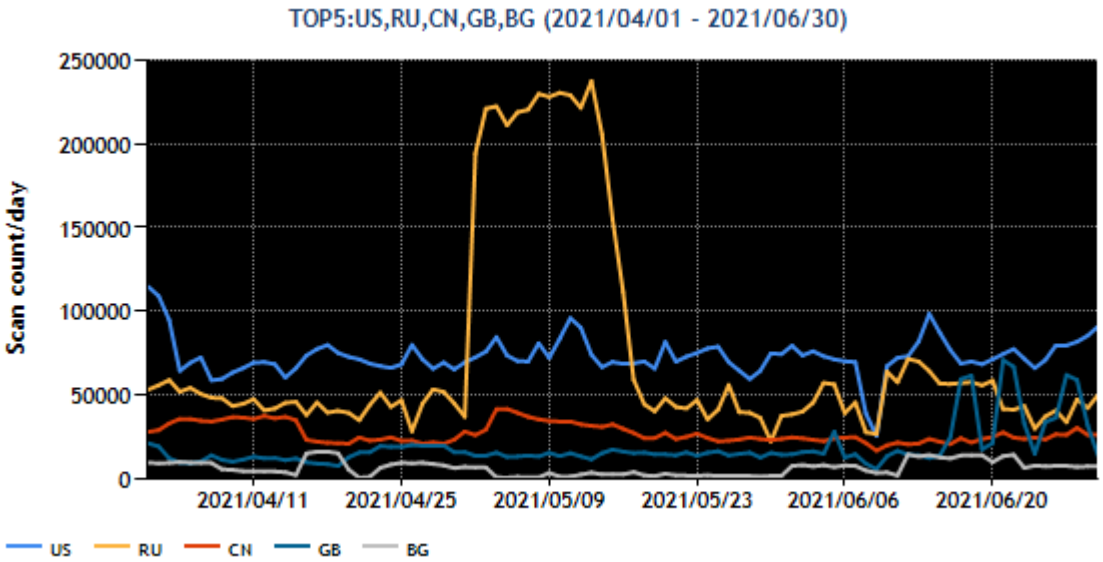
［図 1：2021 年 4～6 月の宛先ポート番号別パケット観測数トップ 5 の推移］

最も多く観測されたパケットは、23/TCP（telnet）宛の通信でした。4 月 13 日に 445/TCP（microsoft-ds）宛のパケットが減少し、4 月 16 日には 123/UDP（ntp）宛のパケットが減少しました。TOP5 には入りませんでしたが、日本国内を送信元としたパケットに注目すると、9530/TCP 宛（全体 18 番目、国内 3 番目）のパケットが期間中多く観測されました。これについては改めて 2.1 で述べます。
次に、本四半期に国内で観測されたパケットについて、送信元 IP アドレスを地域ごとにまとめてパケットが多かった順に並べたトップ 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	1
2	ロシア	2
3	中国	4
4	イギリス	3
5	ブルガリア	9

［表 2］の送信元地域からのパケット観測数の推移を［図 2］に示します。



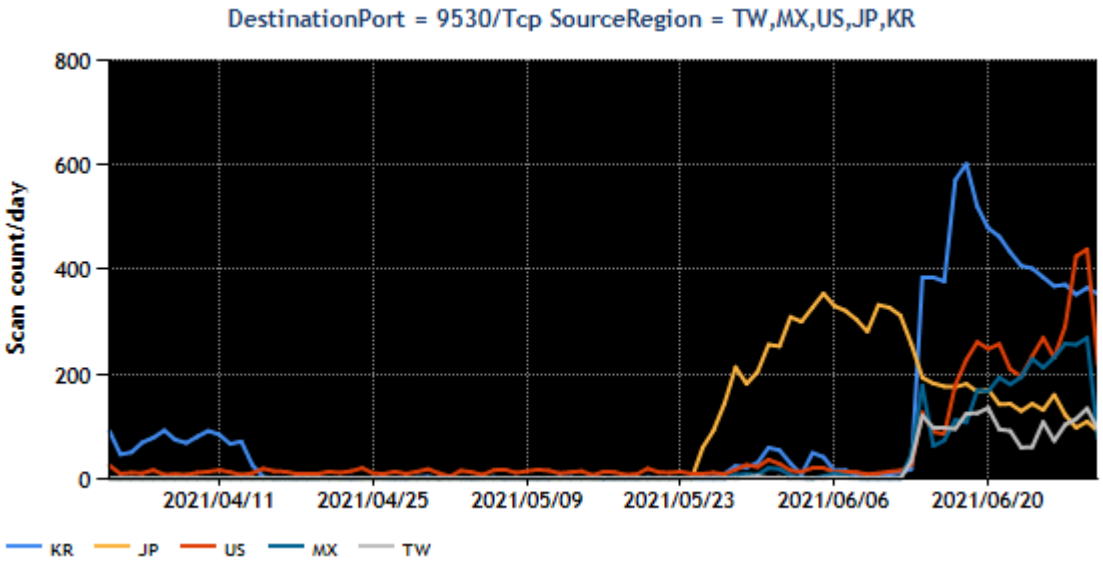
［図 2：2021 年 4～6 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

本四半期に受信したパケットの送信元地域で最も多く見られたのは米国でした。2 番目に多かったロシアからは 5 月 2 日からの 2 週間に他の期間と比較して約 4 倍以上のパケット数を観測しました。これはロシアの少数の IP アドレスを送信元としたパケットをセンサーで観測したためです。サービス提供用に一般的に用いられているポート番号が対象ではなく、さまざまなポートに対するパケットを観測しています。4 番目に多かったイギリスからのパケット数は 6 月以降において増減を繰り返しました。

2. 注目された現象

2.1. Port9530/TCP 宛のパケット数の増加

2021 年 5 月 23 日頃から日本を送信元とした Port9530/TCP 宛のパケットが一時的に多数観測されました（図 3）。6 月 14 日頃からは韓国、米国、メキシコ、台湾などを送信元としたパケットが多く観測されました。日本を送信元としたパケットは期間中 2 番目に多く観測されました。



［図 3：Port9530/TCP 宛のパケット観測数の推移（送信元日本）］

Port9530/TCP 宛のパケットの送信元について、SHODAN 等により 5 月 22 日から 6 月 30 日の間に観測した約 1250 の国内の送信元の IP アドレスについて状況を調べたところ、ロジテック社製ブロードバンドルーターが持つ特徴[2]を確認でき、送信元の約 8 割で脆弱性（CVE-2014-8361）が残されたままインターネットに接続されていることが判明しました。
JPCERT/CC では、インシデント対応の一環として国内の Port9530/TCP 宛のパケットの送信元の IP アドレスの管理者に対して通知を行いました。その結果、一部の管理者から、次のような内容の回答が得られました。

> 「ユーザーに連絡を取りロジテック社製のルーターを利用していることを確認しました。脆弱性への対応が必要な機種のため、別のルーターへの買い替えが必要な旨を案内し、ユーザーから新しいルーターを手配したとの連絡がありました」

JPCERT/CC では、センサーで観測されたパケットの送信元のうち脆弱性（CVE-2014-8361）が解消されていないとみられる送信元に連絡をしています。JPCERT/CC や ISP などから連絡を受けた場合には、ファームウェアのアップデート等のセキュリティ対策にご協力をお願いします。

海外にあるパケットの送信元には、カメラやルーターなどの複数の種類の機器のいずれかが設置されていました。その分布には地域との相関性があまり見られず、海外の一定の地域で広く使用されている機器と推測されます。調査や善処を期待して、各送信元に対応する National CSIRT に情報提供するための準備を進めました。Port9530/TCP 宛のパケットについては 7 月現在も継続しているため、継続して調査を行っていく予定です。

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（2021 年 1～3 月）
https://www.jpcert.or.jp/tsubame/report/report202101-03.html#2.1

本活動は、経済産業省より委託を受け、「令和 3 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。