JPCERT Coordination Center

JPCERT/CC インターネット定点観測レポート

2021 年 7 月 1 日 ～ 2021 年 9 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 **10** 月 **19** 日

JPCERT CC®

目次

1. 概況

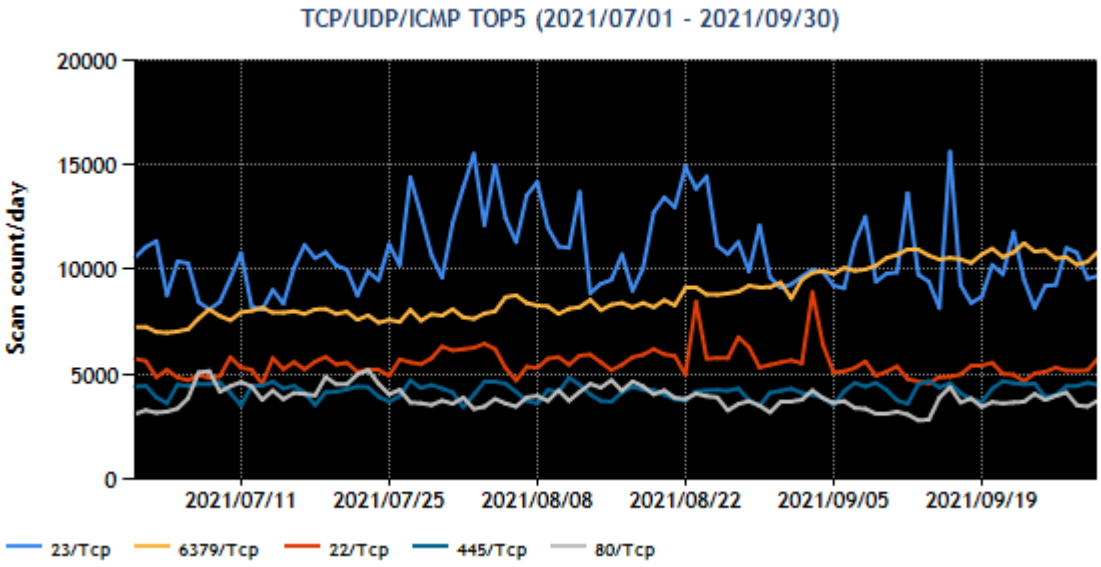
JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、不特定多数に向けて発信されるパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類して、これを脆弱性情報、マルウェアや攻撃ツールの情報などと対比して分析することで、攻撃活動や準備活動の捕捉に努めています。また、こうした観測では、複数の視点からの多元的な見方も重要であるため、主に海外の National CSIRT と連携してそれぞれの組織にセンサーを設置し、観測網に参加してもらう活動を行っています。
各地のセンサーから収集したデータを分析し、問題が見つかれば、適切な地域の National CSIRT などに情報を提供し、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	23/TCP（telnet）	2
2	6379/TCP（redis）	5
3	22/TCP（ssh）	4
4	445/TCP（microsoft-ds）	1
5	80/TCP（http）	7

※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 7～9 月のポート番号宛のパケット観測数トップ 5 の推移］

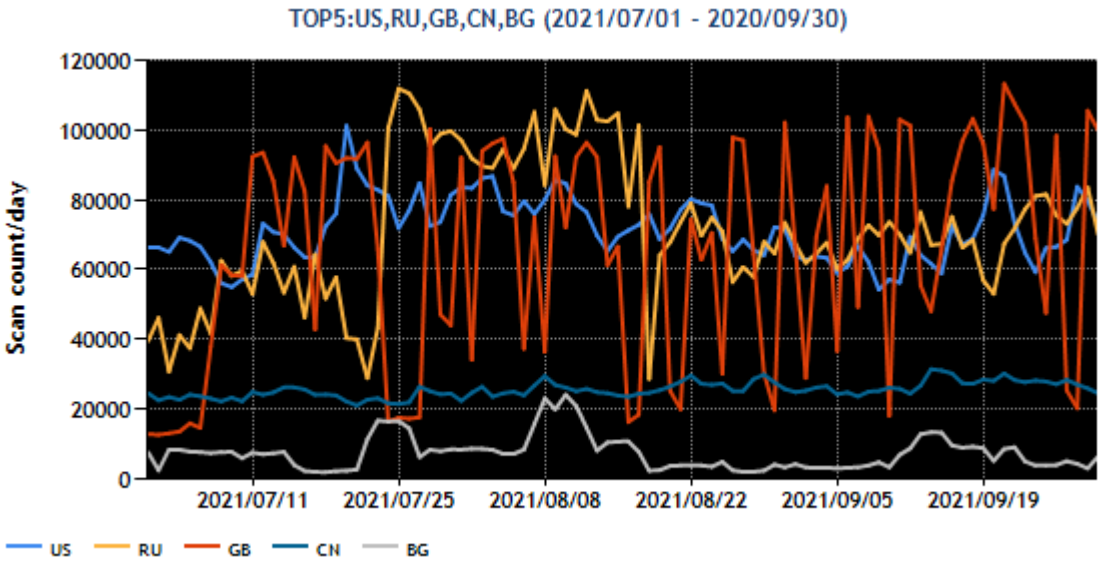
最も多く観測されたパケットは、23/TCP（telnet）宛の通信でした。6379/TCP 宛のパケットが徐々に増加しました。これについては改めて 2.1 で述べます。

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。順位に大きな変動はありませんが、英国は突発的な変化が見られ、順位が入れ替わりました。

［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	英国	4
4	中国	3
5	ブルガリア	5

［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。



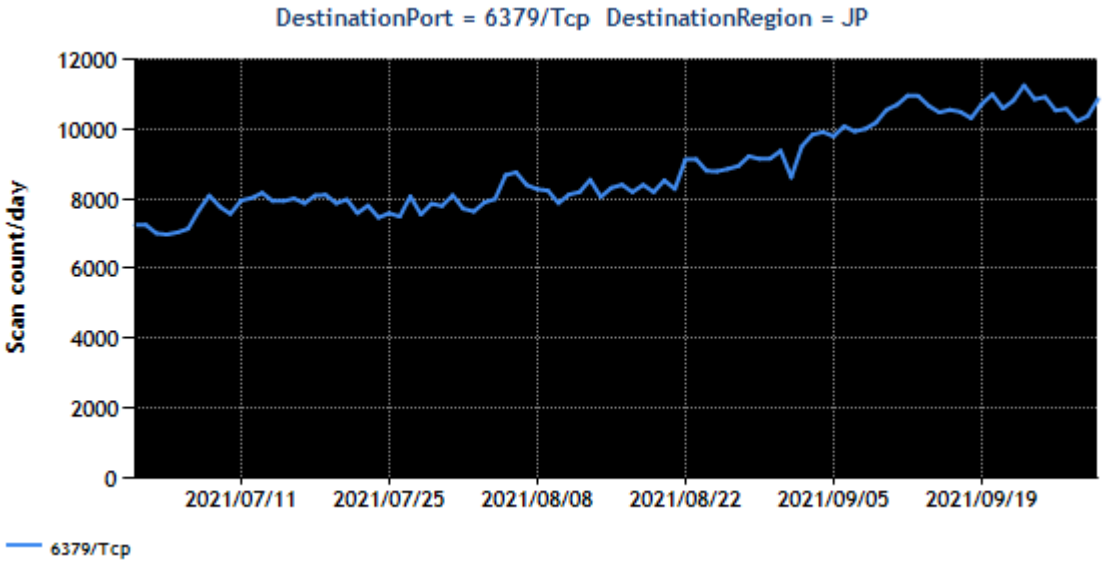
［図 2：2021 年 7～9 月の送信元地域別のパケット観測数トップ 5 の推移］

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、ロシアが 2 番目に続きます。英国は一時的なパケットの増減を繰り返し観測し、中国と順位が入れ替わり 3 番目になりました。中国とブルガリアからのパケットも継続して観測しています。

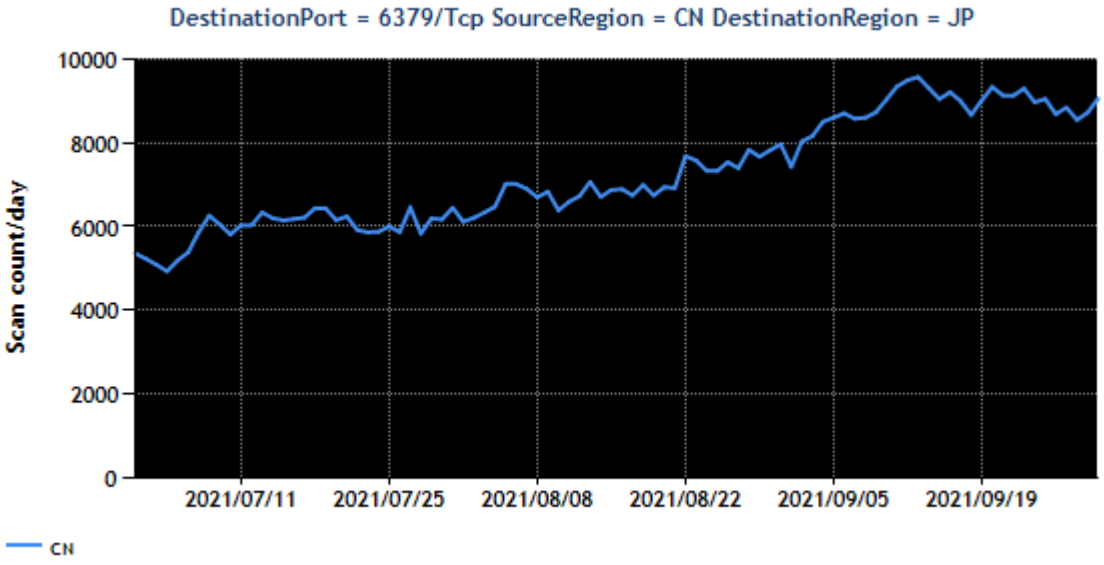
2. 注目された現象

2.1. Port6379/TCP 宛のパケット数の増加

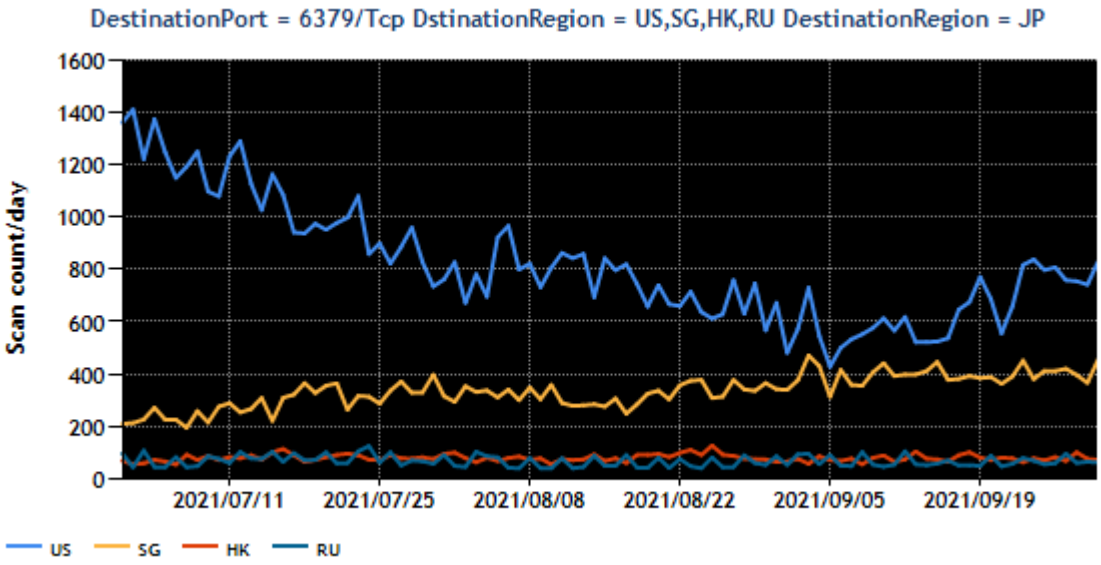
本四半期を通じて 6379/TCP（redis）宛のパケットが観測（図 3）されました。6379/TCP はインメモリデータベース Redis の待ち受けポートとして使用されることが多いポート番号です。
6379/TCP 宛のパケットは、中国を送信元とするパケットが 8 割を超えており、次いで米国、シンガポール、香港、ロシアといった地域からのパケットが観測（図 4、5）されました。



［図 3：Port6379/TCP 宛のパケット観測数の推移］



［図 4：中国を送信元地域とした Port6379/TCP 宛のパケット観測数の推移］



［図 5：中国を除いたトップ 2-4 を送信元地域とした Port6379/TCP 宛のパケット観測数の推移］

中国からの 6379/TCP 宛のパケット数は漸増傾向にあり、本四半期の末日のパケット数は初日の約 1.5 倍になりました。シンガポールからのパケットも同程度の増加率でした。それ以外の地域からのパケットは本四半期を通じて大きな変化は見られませんでした。本四半期は約 20 の国内の IP アドレスから送信された 6379/TCP 宛のパケットも観測されたことから、当該 IP アドレスを管理している事業者に情報を提供したところ、しばらくして送信が止まったことを確認できました。

また、TSUBAME のセンサーで 6379/TCP 宛のパケットを観測した送信元の一部については、不審なリクエストを送信していたことを Redis サーバー（6379/TCP）のハニーポットで確認しています。ペイロードを確認したところ、認証突破や情報の窃取、外部からのファイルの取得、OS に対する操作などが見つかりました。Redis サーバーを運用している方は、サーバーへのアクセス制限や適切な認証が設定されていることの確認や、アクセス状況に関するログの定期的な確認を運用の一環として行うことを推奨します。

パケットの送信元について SHODAN 等のスキャンデータサービスプロバイダーのデータを用いて確認をしたところ、特定の OS やソフトウェアが稼働しているなど共通する要素は見られませんでした。仮に、何らかの脆弱性を対象とした攻撃が行われ、その結果マルウェアに感染したホストから 6379/TCP 宛のパケットが送信されるようになったとすると、日本国内を含むさまざまな地域で 6379/TCP 宛のパケットを送信するホストが増えるはずですが、そうした変化も見られませんでした。そのため、この事象の背景は、マルウェア感染でなく、サーバーが侵入を受けて攻撃の踏み台にされているケースや、攻撃者がインフラを用意しているケースなどに絞られます。それ以上は現在のところ原因がはっきりしていません。いずれにせよ、サーバーの管理者は管理するサーバーに意図しないアクセスなどがないことを確認し、対策を取ることが肝要です。

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

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。