JPCERT Coordination Center

JPCERT/CC インターネット定点観測レポート

2021 年 10 月 1 日 ～ 2021 年 12 月 31 日

一般社団法人 JPCERT コーディネーションセンター

2022 年 **1** 月 **25** 日

JPCERT CC®

目次

1. 概況

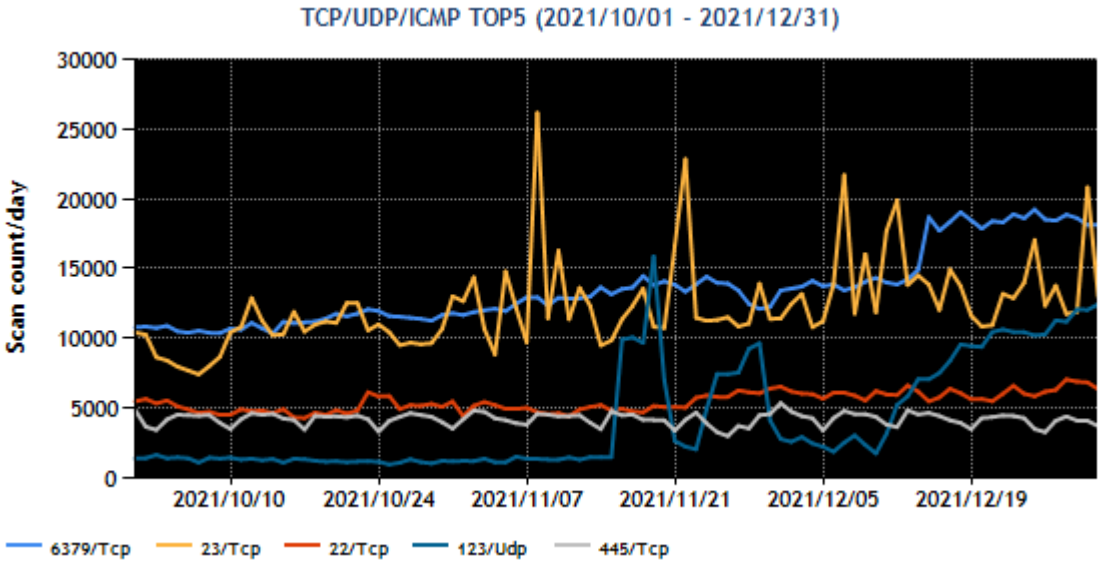
JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、不特定多数に向けて発信されるパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類して、これを脆弱性情報、マルウェアや攻撃ツールの情報などと対比して分析することで、攻撃活動や準備活動の捕捉に努めています。また、こうした観測では、複数の視点からの多元的な見方も重要であるため、主に海外の National CSIRT と連携してそれぞれの組織にセンサーを設置し、観測網に参加してもらう活動を行っています。
各地のセンサーから収集したデータを分析し、問題が見つかれば、適切な地域の National CSIRT などに情報を提供し、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、TSUBAME（インターネット定点観測システム）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	6379/TCP（redis）	2
2	23/TCP（telnet）	1
3	22/TCP（ssh）	3
4	445/TCP （microsoft-ds）	4
5	443/TCP（https）	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 10～12 月のポート番号宛のパケット観測数トップ 5 の推移］

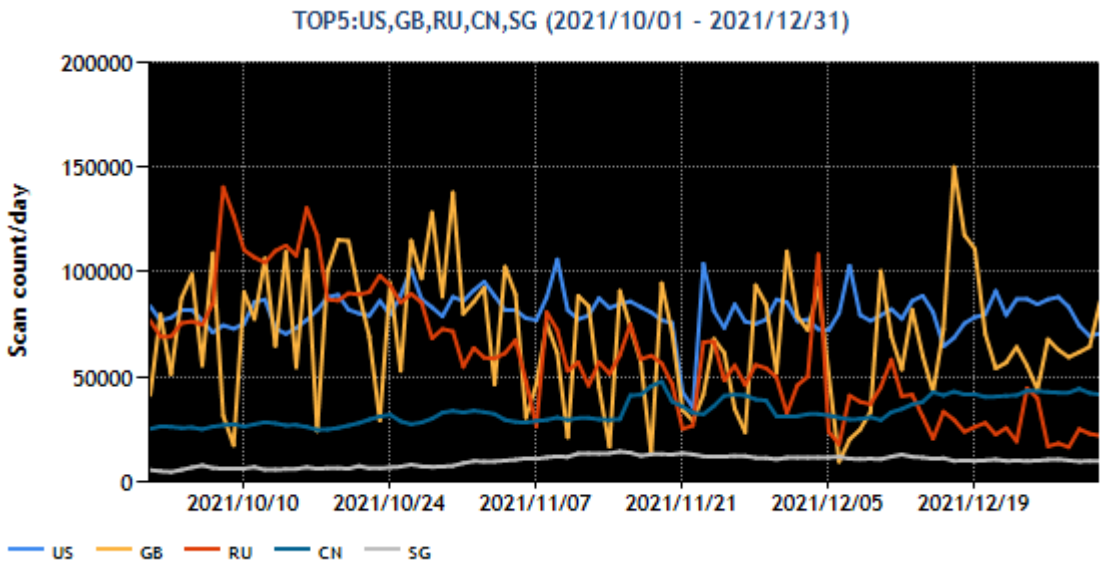
最も多く観測されたパケットは、6379/TCP（redis）宛の通信でした。6379/TCP 宛のパケットは、当該期間で約 1.8 倍に増加しています。6379/TCP 宛のパケットについては改めて 2.1 で述べます。2 番目に多かった 23/TCP は、短期間での増減が複数回発生していました。この背景には、IoT 機器等へマルウェアを感染させようとする攻撃が何度か繰り返し行われ、その度に 23/TCP 宛のパケットの観測数が増加したと考えています。

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	英国	3
3	ロシア	2
4	中国	4
5	シンガポール	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。



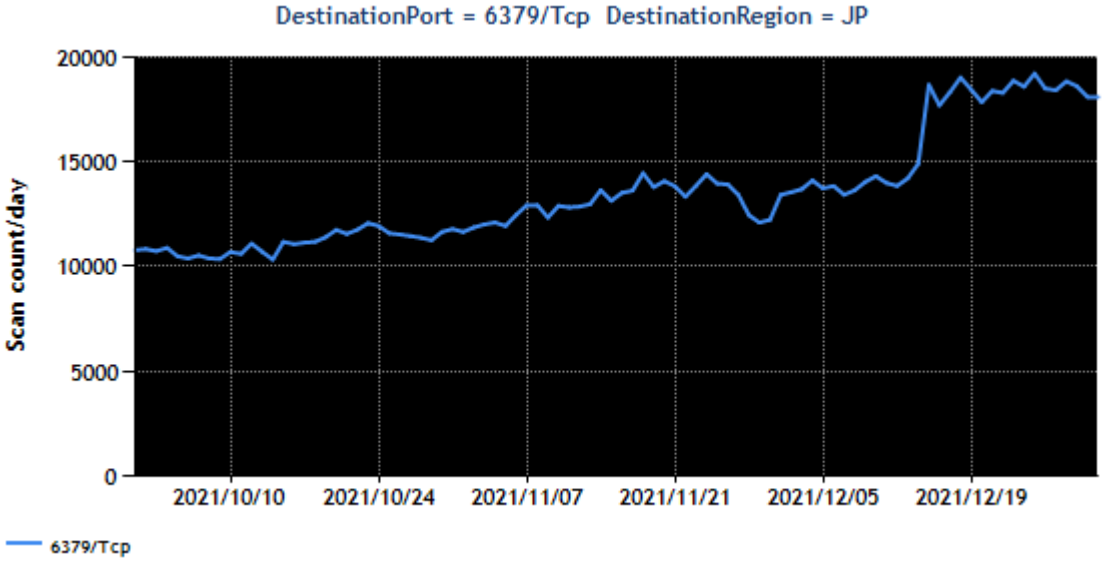
［図 2：2021 年 10～12 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

英国はパケット数が増加し、ロシアと、順位が入れ替わりました。また、シンガポールは 6379/TCP 宛のパケットが増加して 5 番目となるといった順位の変動がありました。

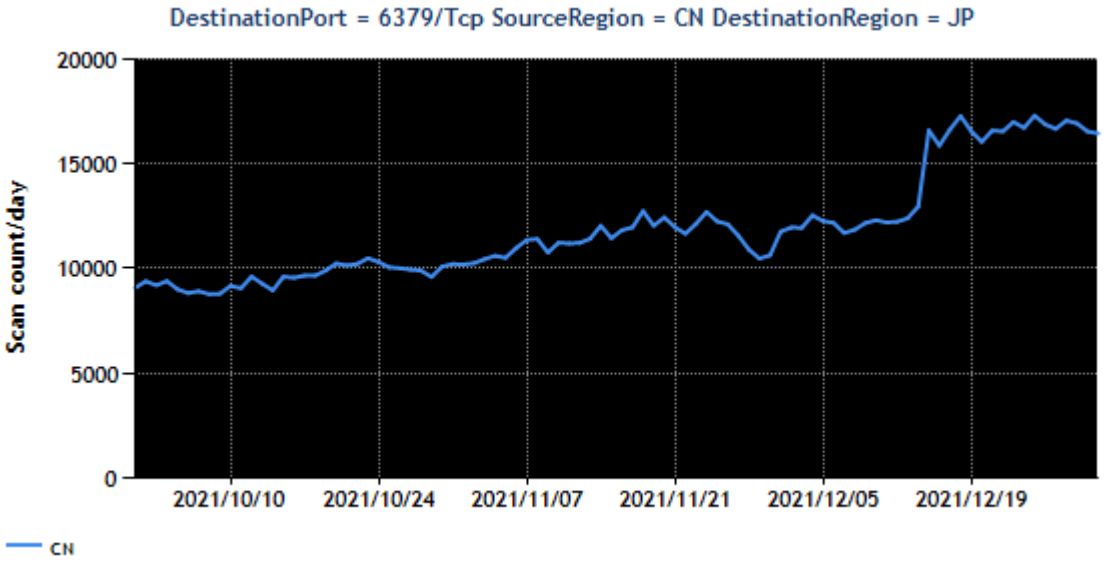
2. 注目された現象

2.1. Port6379/TCP 宛のパケット数の増加

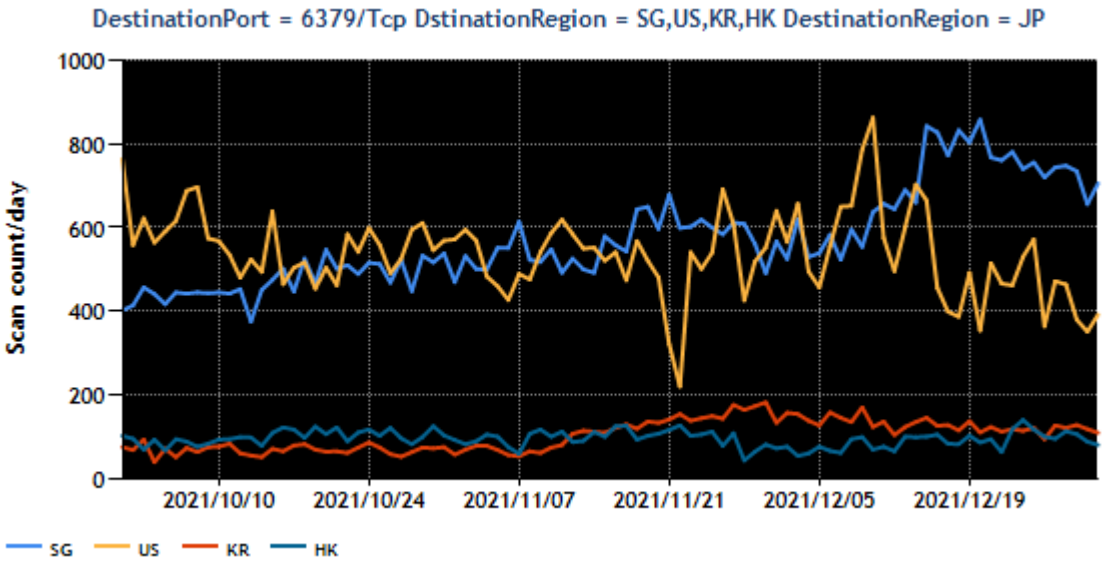
本四半期を通じて 6379/TCP（redis）宛のパケットが多数観測（図 3）されました。6379/TCP はインメモリデータベース Redis の待ち受けポートとして使用されることが多いポート番号です。
6379/TCP 宛のパケットは、中国を送信元とするパケットが 88%を超えており、次いでシンガポール、米国、韓国、香港といった地域からのパケットが観測（図 4、5）されました。
本四半期の中国からの 6379/TCP 宛のパケットは、一時的な減少はあったものの当該期間で約 1.5 倍増加、シンガポールからのパケットは約 1.3 倍増加しています。



［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 TOP2-5 を送信元地域とした Port6379/TCP 宛のパケット観測数の推移］

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。6379/TCP 宛のパケットの全送信元 IP アドレスに占める中国の割合は、前四半期が約 80%(*2)から 88%に増加しました。また、送信元になった IP アドレスの数が増加しています。

送信元が、スキャンだけを行っているのか、実質的な攻撃を行っているかを確認するために、TSUBAME の観測データと JPCERT/CC で運用している Redis を模倣したハニーポットで収集したログを照合してみました。その結果、ハニーポットに一定回数アクセスを行った IP アドレスの集合には、TSUBAME で観測した IP アドレスの集合は重複するものが半数以上あることが分かりました。それらは Redis ハニーポットに対して何らかの処理を行おうとしていたことから、TSUBAME で観測されたパケットの送信元の多くは Redis サーバーを探索するだけでなく、マルウェア感染させようとしていたと推測されます。

6379/TCP 宛のパケットの送信元 IP アドレスについて、対処してもらうためにネットワークを管理している海外の組織に対して、日々、ログなどの情報を提供してきましたが、TSUBAME で確認する限りで状況の明らかな改善には至っていません。そのため、関係地域の CSIRT チームに情報を提供するといった、対処に向けた活動を検討しています。また、日本国内から送信された 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。

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ましたが、特定の OS やソフトウェアが稼働しているといった、パケットの送信元について共通する要素は見つかりませんでした。仮に、何らかの脆弱性を対象とした攻撃の結果、マルウェアに感染したホストがあり、そこから 6379/TCP 宛のパケットが送信されるようになったとすると、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、この攻撃は、自己増殖性を持ったマルウェアを使ったものではなく、侵入したサーバーを踏み台として悪用しているケース、または攻撃者が用意したインフラから行われているケースに絞られます。それ以上は現在のところ分かりません。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、第三者に踏み台として悪用されていないようにすることが肝要です。

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

（2） インターネット定点観測レポート（2021 年 7～9 月）
https://www.jpcert.or.jp/tsubame/report/report202107-09.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。