JPCERT/CC インターネット定点観測レポート

2022 年 10 月 1 日 ～ 2022 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

2023 年 1 月 31 日

目次

1. 概況

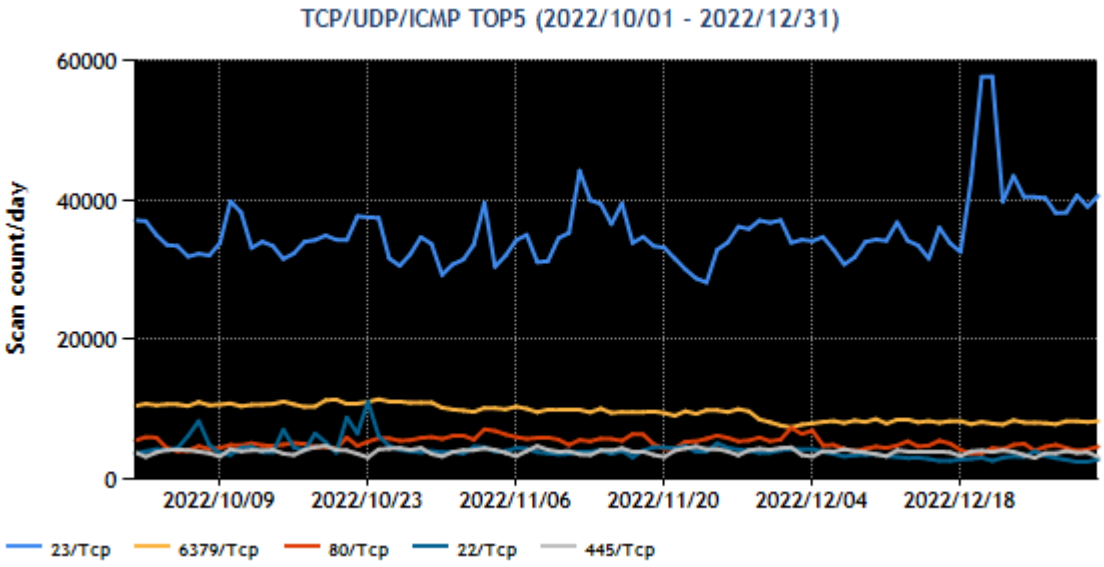
JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、不特定多数に向けて発信されるパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類して、これを脆弱性情報、マルウェアや攻撃ツールの情報などと対比して分析することで、攻撃活動や準備活動の捕捉に努めています。また、こうした観測では、複数の視点からの多元的な見方も重要であるため、主に海外の National CSIRT と連携してそれぞれの組織にセンサーを設置し、観測網に参加してもらう活動を行っています。
各地のセンサーから収集したデータを分析し、問題が見つかれば、適切な地域の National CSIRT などに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



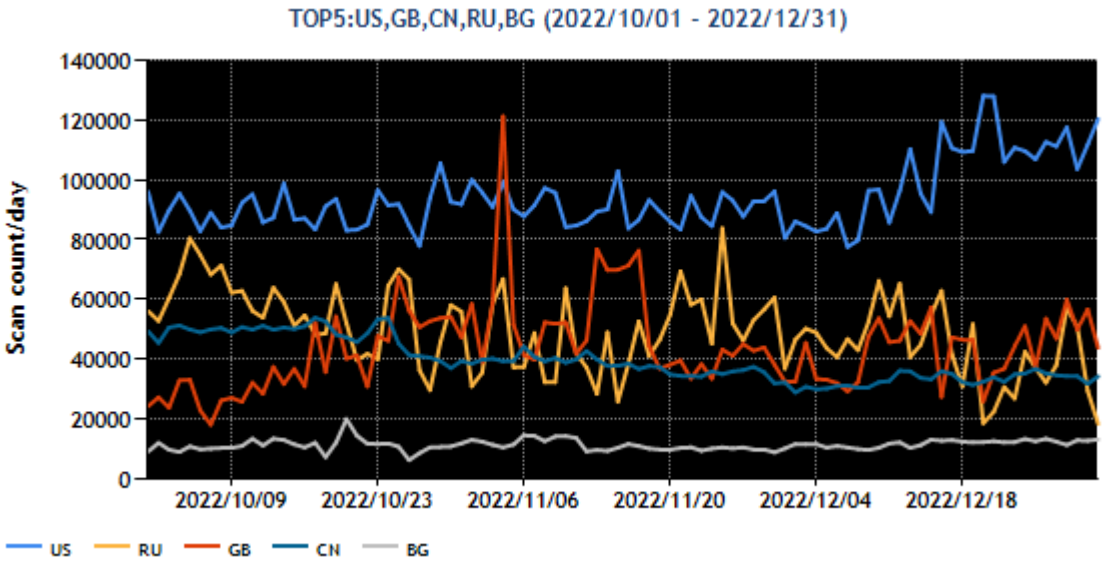
［図 1：2022 年 10～12 月のポート番号宛のパケット観測数トップ 5 の推移］

最も多く観測されたパケットは、23/TCP（telnet）宛で期間中に増減を繰り返していました。6379/TCP 宛のパケットは本四半期も減少傾向が続いています。
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	ロシア	2
3	英国	3
4	中国	4
5	ブルガリア	5

［表 2］に掲げた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。



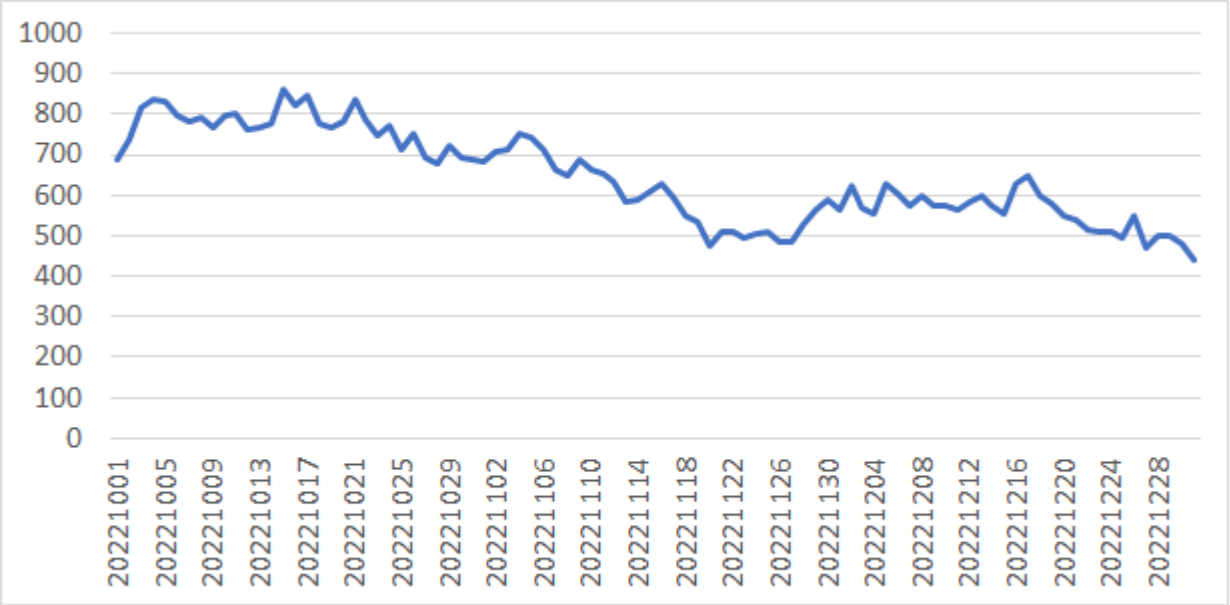
［図 2：2022 年 10～12 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

米国からのパケット観測数が 12 月に入って増加していますが、これは 81/TCP 宛のパケットが増加したことが要因です。また、4 番目に多かった中国は減少傾向にあり、期初と比べて期末には（10 日間平均で）約 2 割減となりました。その他の地域ついて、突発的なパケットの増減はありますが、特筆すべき特徴はなく前四半期と全く同じ送信元地域となったのが特徴です。

2. 注目された現象

2.1. 国内の IoT 機器から送信されたとみられる Mirai の特徴を持つパケットの推移について

期中を通して日本国内の IP アドレスからの Mirai の特徴 （Initial Sequence Number = Destination IP address）を持つパケット（以下「Mirai 型パケット」という。）を観測しました。［図 3］



［図 3：2022 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］

これらのパケットの送信元 IP アドレスの一部について SHODAN を使って送信元の特徴を確認してみました。約 5 割の IP アドレスで DVR やブロードバンドルーターなどの機器が確認でき、一部の製品は、すでに脆弱性情報が公開されている機種でした。例えば、［図 4］に挙げるログイン画面が表示される機器があります。

［図 4：DVR 製品のログイン画面］

このログイン画面を持つ製品は FocusH&S 社製 DVR とみられます。当該製品の脆弱性を狙ってマルウェアに感染させる攻撃活動があることは、NICT のブログ [2] でも紹介されています。
23/TCP や 37215/TCP 宛のパケットなど特徴的な Mirai 型パケットがセンサーで観測されていることから、Mirai の亜種とみられるマルウェアに感染し、スキャンや攻撃活動を行っていると考えられます。国内では、販売代理店の一つであるユニモテクノロジーにて取り扱いがあり、同社から修正済みファームウェアが提供されています。ファームウェアの更新等の対策 [3] をお願いします。
また、Web の管理インタフェースがインターネット上に公開された状態になっていないか、初期パスワードを変更して使用しているか、メーカーの Web サイトからセキュリティ情報が公開されていないか等情報の確認も行ってください。

本四半期は、過去に紹介したロジテック社製のルーターや、Pinetron 社製の DVR とみられる製品が設置されている IP アドレスからも不審なパケットを観測しました。
JPCERT/CC では不審なパケットを観測した際に、ネットワークの管理者にログ情報を提供しています。関係する IP アドレスを保有している組織などから連絡があった際は、機器の状況を確認するようお願いします。

3. 参考文献

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

（2）国立研究開発法人 情報通信研究機構 NICTER Blog
DVR 機器への感染を狙う攻撃の観測
https://blog.nicter.jp/2022/10/analysis-of-ddos-bot-targeting-dvrs/

（3）JVN（Japan Vulnerability Notes）
ユニモテクノロジー製デジタルビデオレコーダにおける重要な機能に対する認証の欠如の脆弱性
https://jvn.jp/vu/JVNVU90821877/index.html

本活動は、経済産業省より委託を受け、「令和 4 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。