JPCERT/CC インターネット定点観測レポート

2023 年 4 月 1 日 ～ 2023 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

2023 年 8 月 16 日

JPCERT CC®

目次

1. 概況

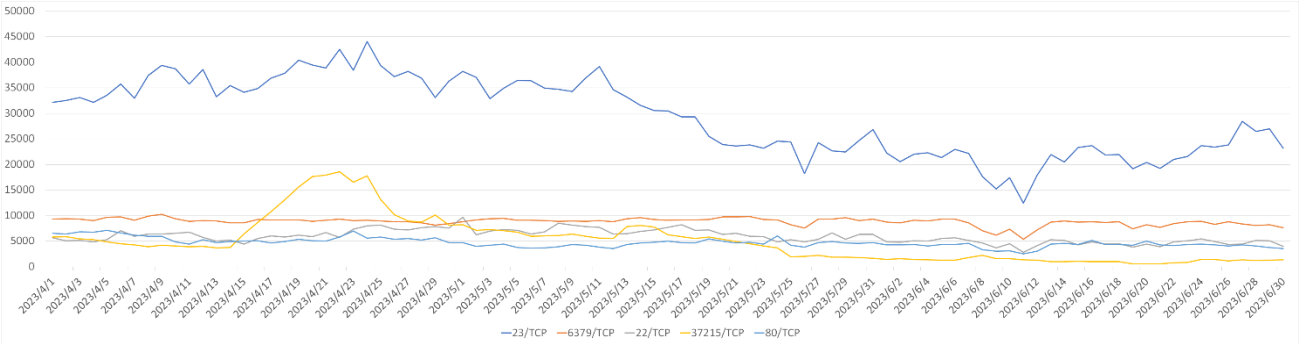
JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、一定の IP アドレス帯に向けて網羅的に発信されるパケットを観測しています。こうしたパケットの発信は特定の機器や特定のサービス機能を探索するために行われていると考えられます。また、JPCERT/CC では、センサーで観測されたパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類して、これを脆弱性情報、マルウェアや攻撃ツールの情報などと対比して分析することで、攻撃活動や準備活動の捕捉に努めています。センサーから収集したデータを分析し、問題が見つかれば、解決できる可能性がある関係者に情報を提供し、善処を依頼しています。
本レポートでは、本四半期に TSUBAME（インターネット定点観測システム）が観測した結果とその分析の概要を述べます。
本四半期に探索されたサービスのトップ 5 は国内において［表 1］に示すとおりでした。

［表 1：頻繁に探索された国内のサービスのトップ 5］

順位	宛先ポート番号	前四半期の順位
1	telnet（23/TCP）	1
2	redis（6379/TCP）	2
3	ssh（22/TCP）	4
4	37215/TCP	3
5	http（80/TCP）	5

※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］に示した探索されたサービスのトップ 5 に対するパケット観測数の推移を［図 1］に示します。



［図 1：2023 年 4～6 月のポート番号宛のパケット観測数トップ 5 の推移］

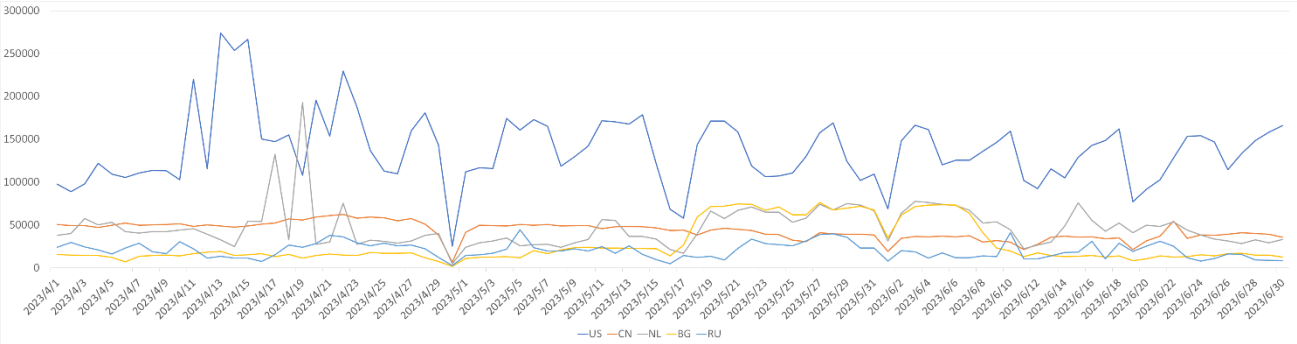
本四半期に最も頻繁に探索されたサービスは telnet（23/TCP）であり、2 番目は redis（6379/TCP）でした。4 番目のポート 37215/TCP の探索は、Mirai の感染活動との関連性が推測できます。Mirai は、感染させることができそうな機器を探索して、それを攻撃して感染させて、新たな攻撃や探索を行うための踏み台とするマルウェアです。この探索活動は、4 月 14 日頃から下旬にかけて大きく増加したのち、何度か増減を繰り返してから、ゆるやかに減少しています。Mirai の特徴（Initial Sequence Number と Destination IP address とが一致する）を持つパケット（以下、Mirai 型パケットという。）はポート 37215/TCP 以外のさまざまなサービスを探索するものがあり、それらの探索の頻度に相関した変動が見られました。その様子を「2.1. 日本を対象とした Mirai の特徴を持つパケットの動向について」にまとめました。

次に、本四半期における国内を対象とした探索活動の探索元について、活動が活発だった地域順に並べたトップ 5 を［表 2］に示します。

［表 2：探索元地域トップ 5］

順位	送信元地域	前四半期の順位
1	米国	1
2	中国	2
3	オランダ	3
4	ブルガリア	6
5	ロシア	4

［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 2：2023 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］

送信元地域について特筆すべき点として、ブルガリアからのパケットが 5 月 18 日頃から 6 月 8 日頃にかけて一時的に増加し、この影響でブルガリアの順位が 3 位に上がりました。それ以外の地域については特筆すべき点がありません。なお、TSUBAME では RIR（Regional Internet Registry）による割り当て情報を用いて個々の IP アドレスの地域を判断しています。

2. 注目された現象

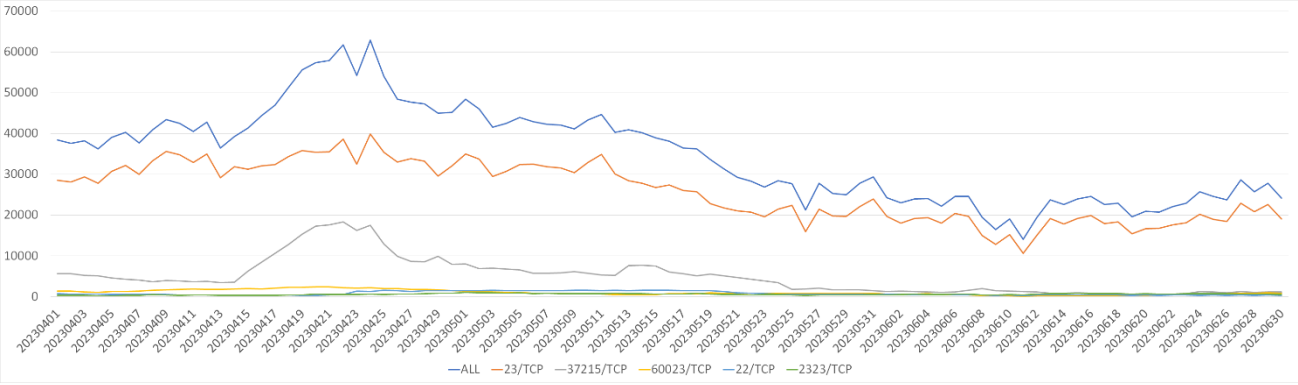
2.1. 日本のセンサーで観測された Mirai 型パケットの動向について

本四半期も、Mirai の感染活動との関連性が推測される特徴を持つパケットが継続的に観測されました。宛先ポート番号を調べると 974 種類あることが分かりました。探索されたポートとそれらの割合を［表 3］に示します。

［表 3：Mirai 型による探索ポートとその割合］

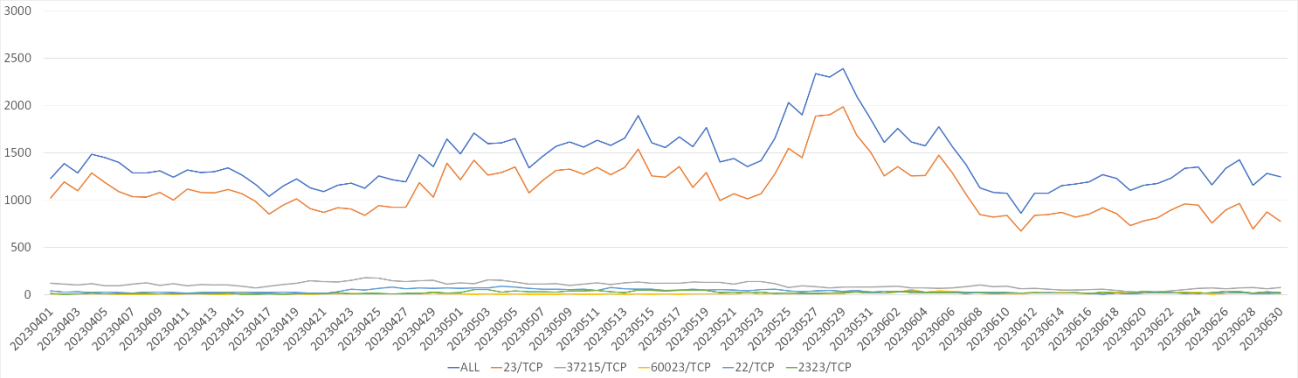
順位	宛先 Port 番号	割合
1	23/TCP	74.08%
2	37215/TCP	14.27%
3	60023/TCP	3.01%
4	22/TCP	2.25%
5	2323/TCP	1.79%
6	52869/TCP	0.88%
7	5555/TCP	0.67%
8	56575/TCP	0.65%
9	80/TCP	0.51%
10	2222/TCP	0.38%
TOP10 外		1.51%

Mirai 型パケットが探索しているサービスの 74%が telnet（23/TCP）でした。どのサービス探索の頻度にも目立った変化がありました。［表 3］に示した、各地域を送信元とするパケットと宛先 Port 番号すべてを合算したパケットの観測数の推移を［図 3］に示します。



［図 3：探索元海外の Mirai の特徴を持つパケットの推移］

37215/TCP 宛のパケットは、4 月 14 日頃から増え、4 月 20 頃のピーク以降は減ってきています。
60023/TCP 宛のパケットについても 4 月 20 日頃をピークにゆるやかに減少しました。
次に、Mirai 型パケットにより日本から行われた探索数の推移を［図 4］に示します。



［図 4：探索元日本の Mirai の特徴を持つパケットの推移］

海外からの探索と日本からの探索を比較すると、どちらも頻繁に探索されたサービスは、telnet（23/TCP）が本四半期を通じて最も多いことが分かりました。また、37215/TCP については、国内からの探索（［図 4］参照）が 4 月に僅かに増えたものの、海外からの探索（［図 3］参照）には目立った変化がなく、その後はいずれも徐々に減っていきました。
60023/TCP 宛のパケットについては、4 月に小規模な増減があり、5 月中旬からは増加した状態が続いています。これらの変化は攻撃対象として探索されている機器の機種が変わっている影響と考えられます。
以上に述べたように、攻撃者が Mirai 由来のコードを使用し探索対象とする機器を変化させながら機器の探索や攻撃を行いマルウェアの感染をさせていると推測し、攻撃者が狙っている機器の変化を明らかにする目的で、探索対象のサービスの時間的な変化の分析を試みましたが、その結果からは攻撃対象機器の変化を読み取ることはできませんでした。
しかしながら、Mirai 由来のコードを使用した攻撃は現在も継続されており、さまざまなサービスの探索が行われています。その実像に迫るために、国内の探索元の IP アドレスについては調査を行い、どのような機器がこの探索に関与しているのかを解明することを試みました。この調査から、探索元の一部について、そこで動作している機種をほぼ特定することができました。脆弱性が存在する古い家庭用向け無線 LAN ルーターや DVR 製品でした。見つかった問題のある機器については、JPCERT/CC のインシデント対応窓口を通じて、ISP のアビューズ窓口等へ情報を提供し、ユーザーに善処を求めるよう依頼しました。

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 5 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。