JPCERT Coordination Center

JPCERT/CC インターネット定点観測レポート

2022 年 1 月 1 日 ～ 2022 年 3 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 4 月 21 日

JPCERT CC®

目次

1. 概況

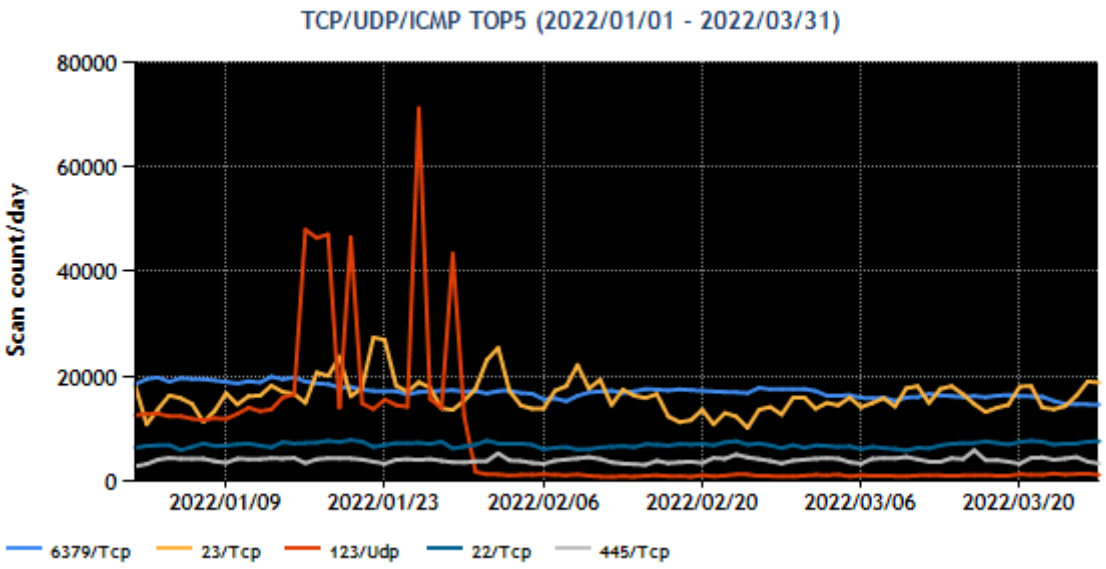
JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、不特定多数に向けて発信されるパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類して、これを脆弱性情報、マルウェアや攻撃ツールの情報などと対比して分析することで、攻撃活動や準備活動の捕捉に努めています。また、こうした観測では、複数の視点からの多元的な見方も重要であるため、主に海外の National CSIRT と連携してそれぞれの組織にセンサーを設置し、観測網に参加してもらう活動を行っています。
各地のセンサーから収集したデータを分析し、問題が見つかれば、適切な地域の National CSIRT などに情報を提供し、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）	1
2	23/TCP（telnet）	2
3	123/UDP（ntp）	6
4	22/TCP（ssh）	3
5	445/TCP（microsoft-ds）	4

※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 1～3 月のポート番号宛のパケット観測数トップ 5 の推移］

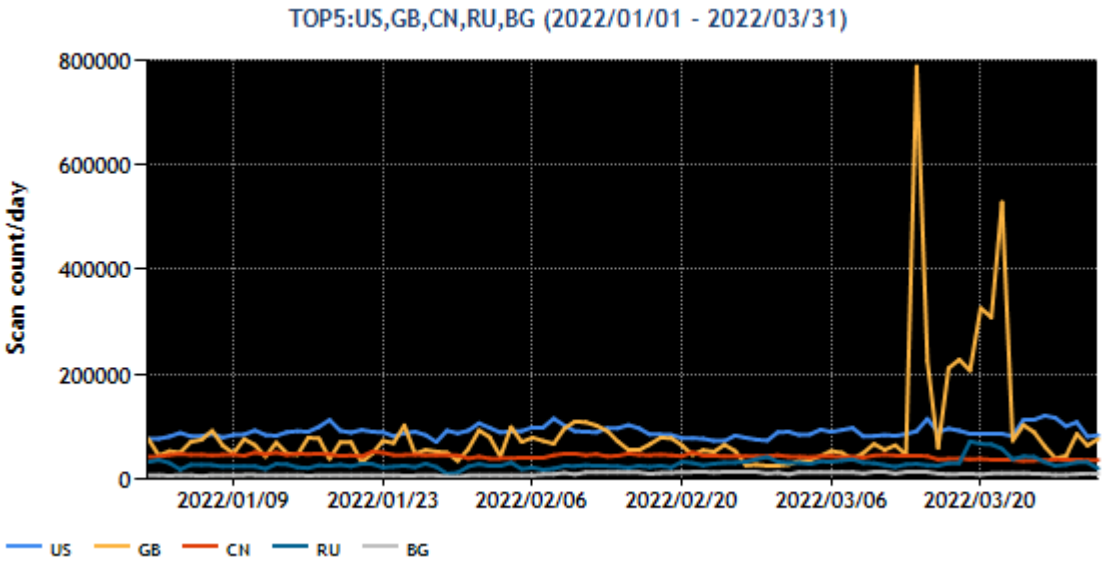
最も多く観測されたパケットは、6379/TCP（redis）宛の通信でした。6379/TCP 宛のパケットは、当該期間では、緩やかに減少しているように見え、期初と期末で比較すると約 20%減少していました。2 番目に多かった 23/TCP は、短期間での増減が複数回発生していました。この背景には、IoT 機器等をマルウェアに感染させようとする攻撃が何度か行われ、その度に 23/TCP 宛のパケットの観測数が増加したのではないかと考えています。

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	2
3	中国	4
4	ロシア	3
5	ブルガリア	6

［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。



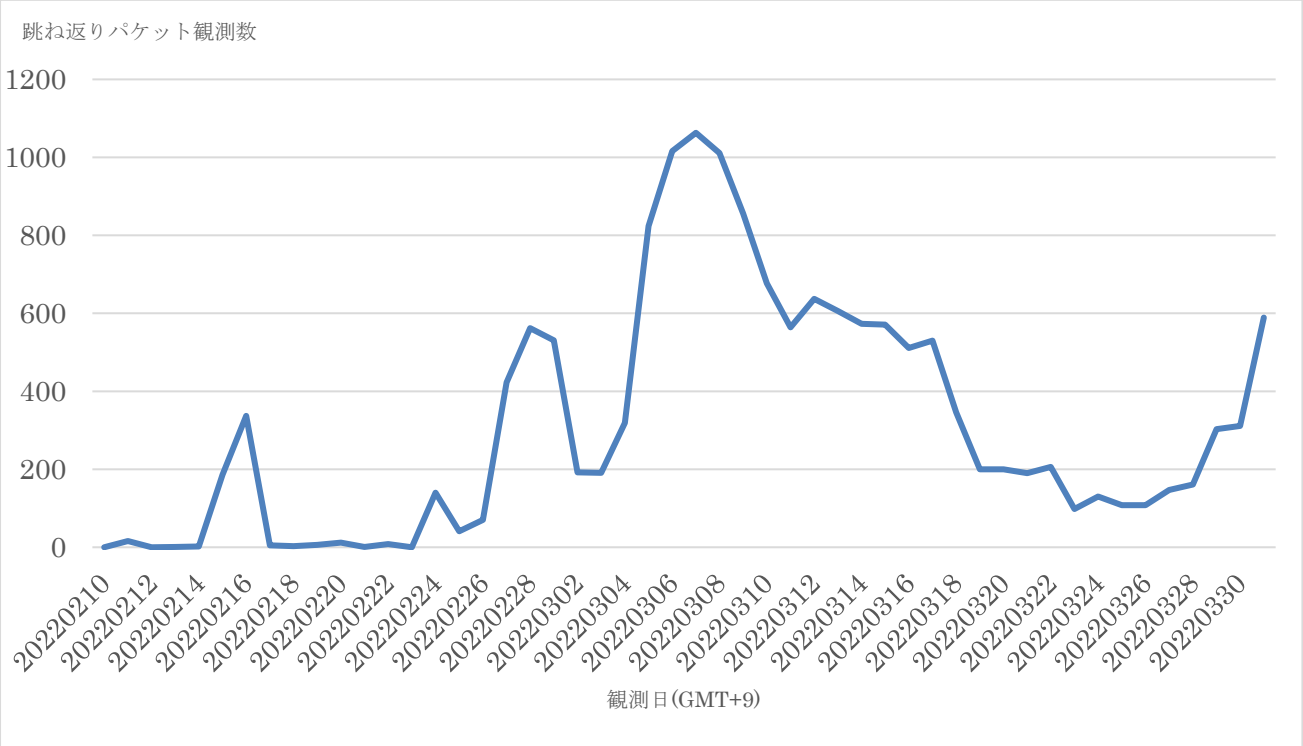
［図 2：2022 年 1～3 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

英国からのパケットについて 3 月中旬に急激な増加が数回観測されました。RECYBER PROJECT NETBLOCK を送信元としたパケットで短時間に多数のポート宛のパケットを観測しました。シンガポールからのパケットは減少し、ブルガリアと順位が入れ替わりました。

2. 注目された現象

2.1. ウクライナを送信元地域とした跳ね返りパケット数の増加

2 月中旬頃からウクライナを送信元地域とした TCP パケットであって、DDoS 攻撃を受けた際にみられる SYN と ACK フラグがセットされたものを観測しました。（図 3）
TSUBAME になりすまして、すなわち TSUBAME のセンサーの IP アドレスを送信元アドレスに設定して、攻撃対象とするサーバーに SYN フラグをセットしたパケットが送られていて、攻撃対象のサーバーが応答として SYN、ACK フラグをセットして送り返しているパケット（以下、跳ね返りパケット）であると推測しています。こうした跳ね返りパケットは、DDoS 攻撃の手法の一つである Syn flood 攻撃に際し観測されます。



［図 3：ウクライナを送信元地域とした跳ね返りパケットの観測数の推移］

DDoS 攻撃を受けているとのコメントが 2 月 15 日に SNS 上[2]でウクライナから発せられています。2 月 15 日頃に観測された跳ね返りパケットの送信元アドレスの中に、ウクライナで Web サーバーとして利用されているノードの IP アドレスが確認できました。また、攻撃のターゲットとなっていた Port 番号は 80/TCP と 443/TCP でした。
国内外のセキュリティベンダーの情報[3]では、複数の手法の DDoS 攻撃も行われているとされており、その一部の余波である跳ね返りパケットが TSUBAME で観測されたのであろうと考えています。
こうした跳ね返りパケットを 2 月 15 日以後も継続して観測しており、ウクライナを対象とした DDoS 攻撃が継続して行われていると思われます。外部データから調査できたものについて、主な攻撃対象を表 3 に記します。

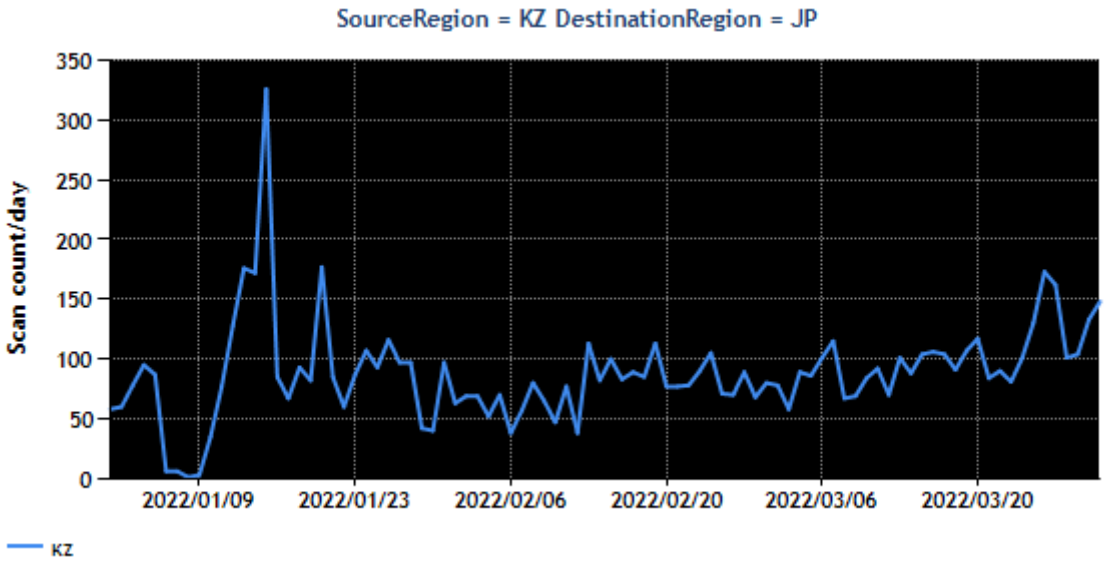
［表 3：跳ね返りパケットの送信元とみられる組織］

Office of the Verkhovna Rada of Ukraine
Office of the President of Ukraine
Ukrainian National Information Agency
State Special Communications Service of Ukraine
PrivatBank
State Savings Bank of Ukraine
TASCOMBANK
Kharkov Metropolitan
Ukrainian Media Holding
Naftogaz Of Ukraine
金融機関向けサービスとソフトウェアを提供する会社
ニュースサイト
固定回線 ISP・携帯電話会社
ホスティング業者
CDN 事業者

JPCERT/CC では、ウクライナの CERT-UA に対し観測動向に関する情報を提供しました。

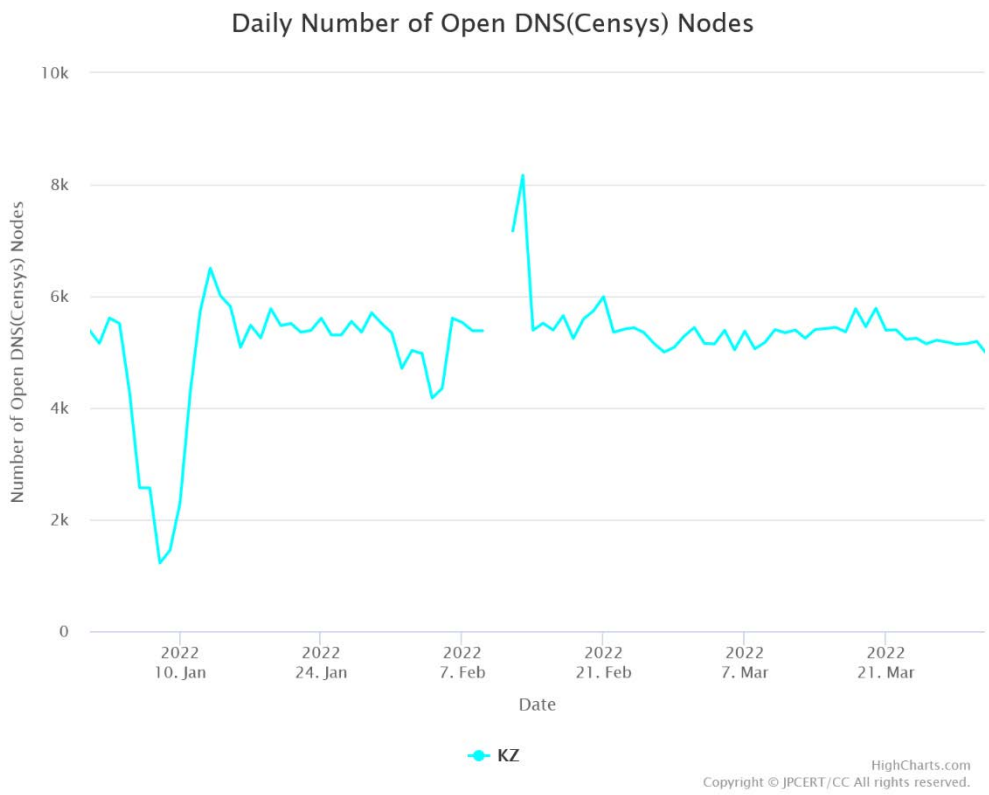
2.2. カザフスタンを送信元地域としたパケット数の一時的な減少について

TSUBAME センサーに届くパケットは、送信元の状況だけでなく、パケットが通過する経路の状況の変化の影響も受けます。つまり、送信元の状況に大きな変化がなくとも、例えばパケットの通信経路が遮断ないし不安定になれば、観測されるパケット数が減少します。
2022 年 1 月 5 日から 10 日にかけて、送信元地域がカザフスタン（KZ）となっているパケットの観測数が減少しました。（図 4）

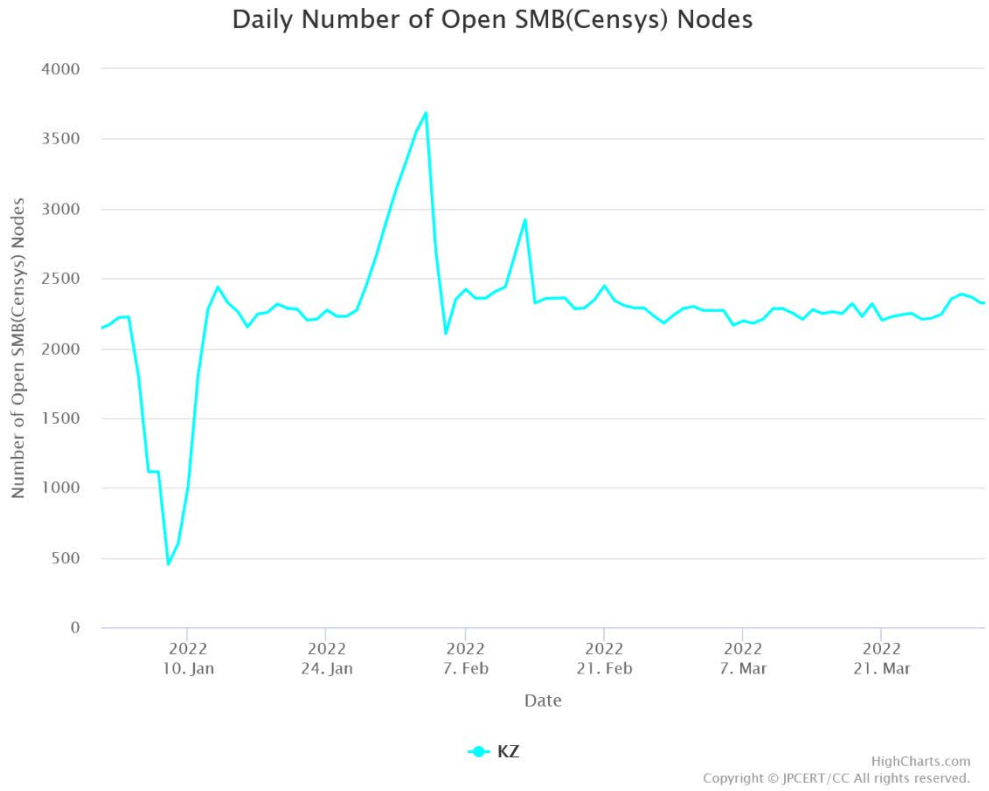


［図 4：カザフスタンを送信元地域としたパケットの観測数の推移］

カザフスタンでは 1 月 1 日に発表された液化石油ガスの価格に対してデモ活動が行われ、その後全土に拡大していったとの報道[4]がありました。1 月 5 日には大統領が非常事態宣言を全土に拡大、集団安全保障条約機構（CTSO）に治安維持部隊の出動を要請するといった事象がありました。
サイバーセキュリティとインターネットのガバナンスの状況を監視している非政府組織の NetBlocks では、インターネットが 1 月 5 日から 1 月 10 日にかけて全土で遮断された[5] [6]と推測しています。
JPCERT/CC がインターネットリスクの可視化を目的に行っている実証実験プロジェクト Mejiro では、インターネット上のノードがインターネットからアクセス可能な状態になっているものについて、Mejiro 指標として公開しています。Mejiro ではクローラが収集したデータ UTC で集計して使用していますが、1 月 5 日から 10 日にかけて、オープンリゾルバーの観測数などが減少（図 5、図 6）しています。



［図 5：カザフスタンのオープンリゾルバーノード数の推移］



［図 6：カザフスタンのオープン SMB ノード数の推移］

TSUBAME および Mejiro による観測データでは一時的な変化であったことを踏まえると、カザフスタン内のボットネットの活動や、オープンリゾルバーの状況の変化というよりも、通信制限による影響の一端ではないかと推測しています。

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） Defence of Ukraine
https://twitter.com/DefenceU/status/1493628291844083723

（3） 360 Netlab
https://twitter.com/360Netlab/status/1493797519725367302

（4） 燃料価格に対する抗議デモを機に、マミン首相が辞職
https://www.jetro.go.jp/biznews/2022/01/d97c27fec4aaf775.html

（5） NetBlocks
https://twitter.com/netblocks/status/1480713969295933443

（6） Kazakhstan’s Internet Shutdown Offers Lessons for Russia-Ukraine Crisis
https://www.nytimes.com/2022/02/18/technology/kazakhstan-internet-russia-ukraine.html

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。