JPCERT CC®

JPCERT Coordination Center

JPCERT/CC インターネット定点観測レポート

2020 年 7 月 1 日 ～ 2020 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

2020 年 10 月 29 日

目次

1. 概況

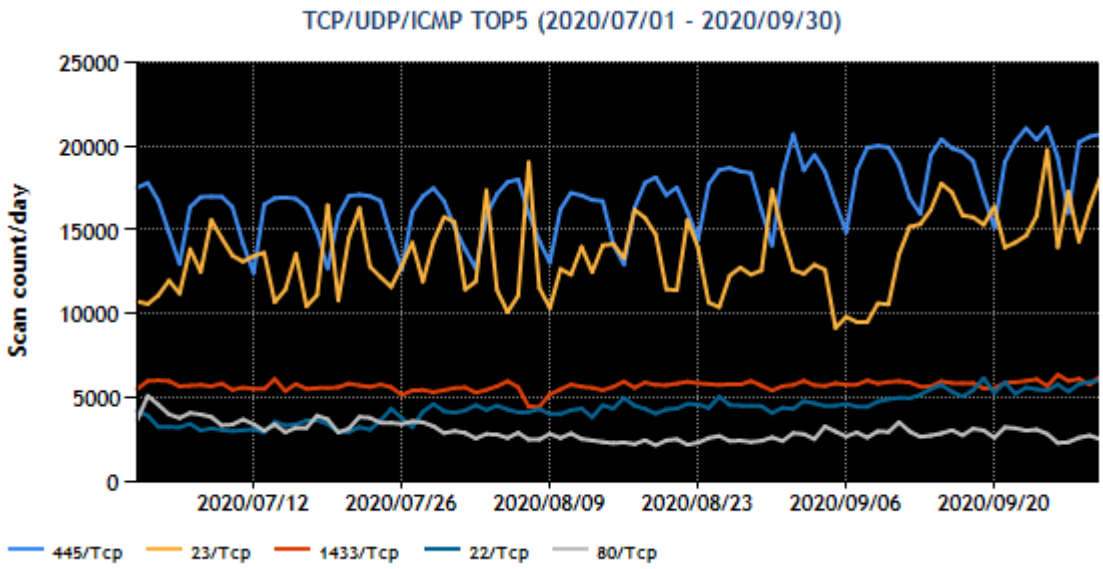
JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、不特定多数に向けて発信されるパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類して、これを脆弱性情報、マルウェアや攻撃ツールの情報などと対比して分析することで、攻撃活動や準備活動の捕捉に努めています。また、こうした観測では、複数の視点による多元的な見方も重要であるため、主に海外の National CSIRT と連携してそれぞれの組織にセンサーを設置し観測網に参加してもらう活動を行っています。
各地のセンサーから収集したデータを分析し、問題が見つかれば、適切な地域の National CSIRT などに情報を提供し、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、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るとトップ 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	445/TCP (microsoft-ds)	2
2	23/TCP (telnet)	1
3	1433/TCP (ms-sql)	3
4	22/TCP (ssh)	5
5	80/TCP(http)	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則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もつパケット観測数の推移を［図 1］に示します。



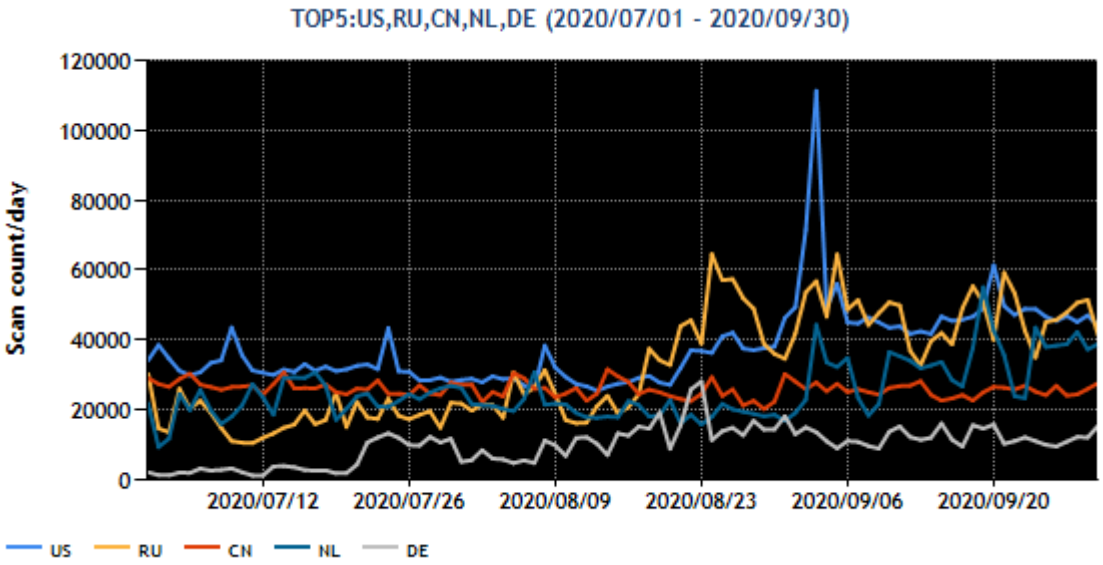
［図 1：2020 年 7～9 月の宛先ポート番号別パケット観測数トップ 5 の推移］

最も多く観測されたパケットは、445/TCP（microsoft-ds）宛の通信でした。4 月下旬から増加した状態が継続しています。また、22/TCP（ssh）宛のパケットが増加傾向で、送信元ホスト数も増加しています。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	2
2	ロシア	1
3	中国	4
4	オランダ	3
5	ドイツ	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。



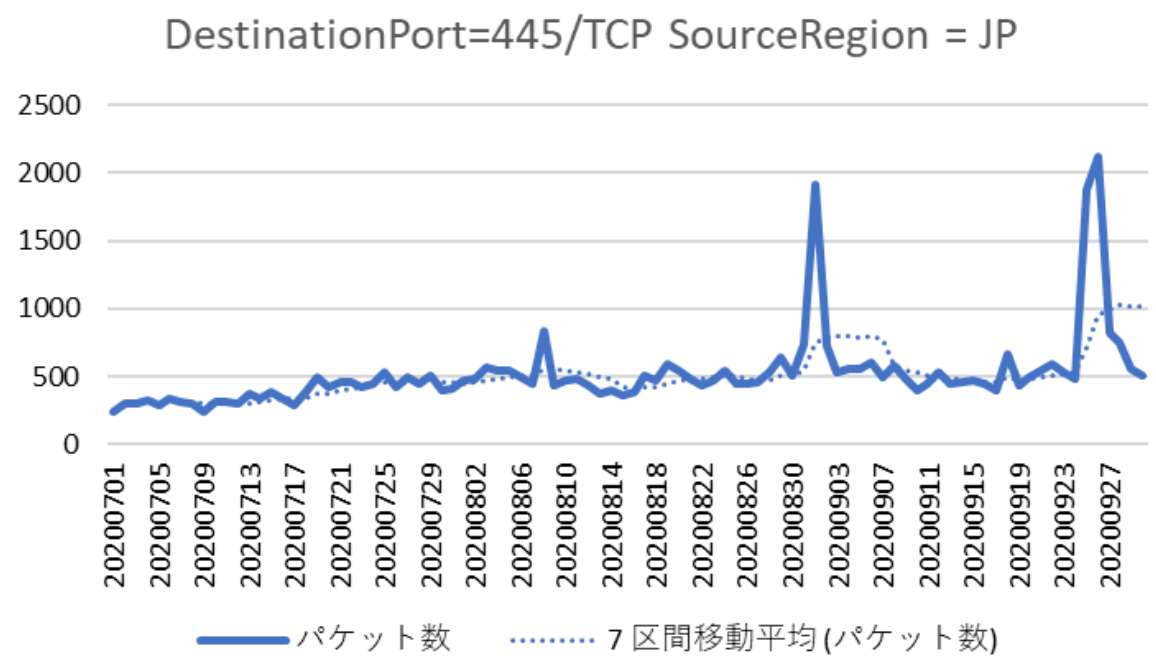
［図 2：2020 年 7～9 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

本四半期に受信したパケットの送信元地域として、最も多く見られたのは米国でした。米国を送信元地域としたパケットの TOP5 の宛先ポート番号は、他の地域と大きな違いはありません。2 位のロシアから届いたパケットでは 22/TCP 宛が最も多く、3389/TCP がそれに次いでいました。その二つの宛先ポートへのパケット観測数は、他の地域と比較して 1 割以上多く、また時期的な増減の様子も異なっています。その他の地域については、順位に大きな変化はありません。

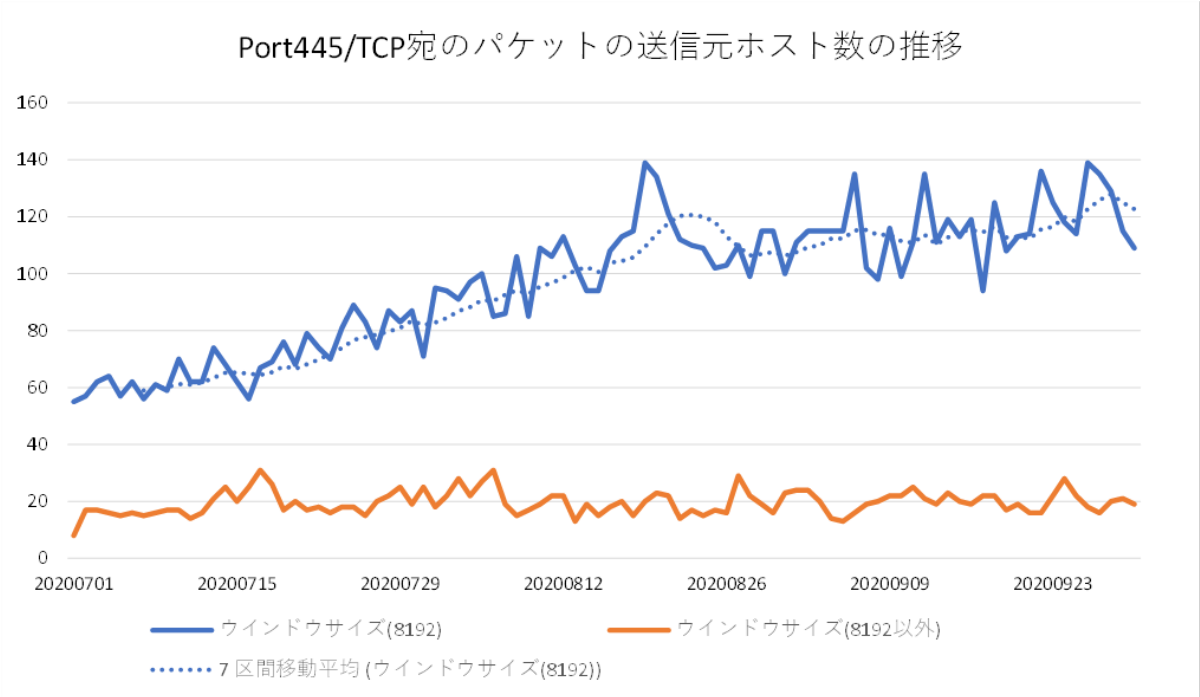
2. 注目された現象

2.1. 送信元が日本となっている Port445/TCP 宛のパケット数の増加

本四半期を通して、送信元が日本となっている 445/TCP 宛のパケット数およびホスト数が一時的な急増を伴いつつ基調として増加傾向にあります。（図 3、図 4）



［図 3：Port445/TCP 宛のパケット観測数の推移（送信元日本）］



［図 4：Port445/TCP 宛のパケットの送信元ホスト数の推移（送信元日本）］

観測されている 445/TCP 宛のパケットには TCP パケットのウインドウサイズに特徴があります。送信元の一部を確認したところ、複数の Windows OS が確認できましたが、特定のバージョンやマシンの利用用途に偏っているといった特徴は見られませんでした。送信元の IP アドレスの管理者に連絡を行なったところ、サポートが終了したバージョンの Windows サーバーが動作していたとの返事を受け取ったケースもありました。返事によれば、侵害されたサーバー上でマイニングマルウェアの動作や、他のホストを MS17-010 の脆弱性を使用して攻撃する挙動がみられたとのことです。観測されている 445/TCP 宛のパケットの多くは特定のウインドウサイズを持っていました。図 4 に示すようにウインドウサイズが 8192 となっているパケットの送信元ホスト数が増加傾向にあります。8192 以外の値となっているパケットの送信元ホスト数には大きな変化が見られません。ウインドウサイズの 8192 は MS17-010 の脆弱性を悪用していることで知られるマルウェアが発するパケットの特徴と一致しています。
2020 年 9 月末以降も、IP アドレスの管理者への連絡とともに、当該ポート宛のパケットの観測を継続しています。Windows を搭載したマシンの管理者の皆様には、サポート期間が終わったバージョンや、不要なポートがネットワークに対して開いた状況になっていないか、アップデートなどの対策が適切に実施され、適切な強度のパスワードが設定されているかなどの確認をお勧めします。

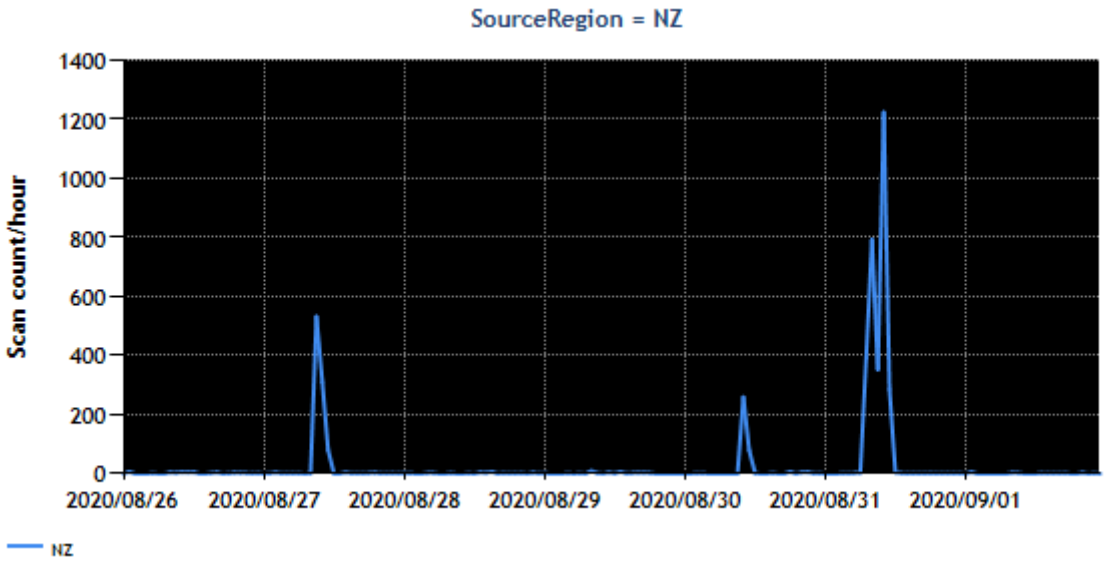
2.2. DDoS 攻撃の一部と推測されるパケットの観測について

8 月 27 日と 8 月 30 日、8 月 31 日にニュージーランドを送信元とした一時的なパケットの増加を観測しました。この時期にはニュージーランド証券取引所やニュージーランド銀行が DDoS 攻撃を受けていると報道[2]されていました。今回観測したパケットは、DDoS 攻撃に関連したパケットに共通に見られる特徴をもち、攻撃の試行や攻撃の結果によるものと考えられます。観測結果を［表 3］と［図 5］に示します。

［表 3：TSUBAME で通信を確認した送信元 IP アドレス数］

日付	送信元 IP アドレス数（注 1）	IP アドレス保有組織（注 2）
2020 年 8 月 27 日	4	ニュージーランド証券取引所
2020 年 8 月 30 日	1	ニュージーランド証券取引所
2020 年 8 月 31 日	7	ニュージーランド銀行

（注 1）TSUBAME に届いたパケットにおいて一定数以上見られた送信元 IP アドレスの数
（注 2）WHOIS に基づいて特定された IP アドレス保有組織



［図 5：8 月 26 日～9 月 2 日にかけてのニュージーランドからのパケットの推移］

これらの IP アドレスから届いたパケットは次の 2 種類のいずれかでした。

- 特徴 1
  - 送信元 Port 番号が 443/TCP
  - ウインドウサイズがある数値で固定
  - シーケンス番号がある数値で固定

- 特徴 2
  - 送信先 Port 番号が 23/TCP
  - ウインドウサイズがある数値で固定

JPCERT/CC ではこれらの観測事象および特徴を、ニュージーランドの National CSIRT（NZ-CERT）に連絡しました。

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

(2) Unprecedented: DDoS Attacks Take Down NZ Stock Market, Banks, Online News & Weather Service
https://secalerts.co/article/unprecedented-ddos-attacks-take-down-nz-stock-market-banks-online-news--weather-service/444f8e80
DDoS Attacks on New Zealand Stock Exchange Highlight Global Spike in ISP Assaults
https://www.msspalert.com/cybersecurity-markets/asia-pacific/ddos-attacks-on-new-zealand-stock-exchange-highlight-global-spike-in-isp-assaults/

本活動は、経済産業省より委託を受け、「令和２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。