JPCERT/CC インターネット定点観測レポート

2019 年 4 月 1 日 ～ 2019 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

2019 年 7 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、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、マルウエ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 等に情報を提供し、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。

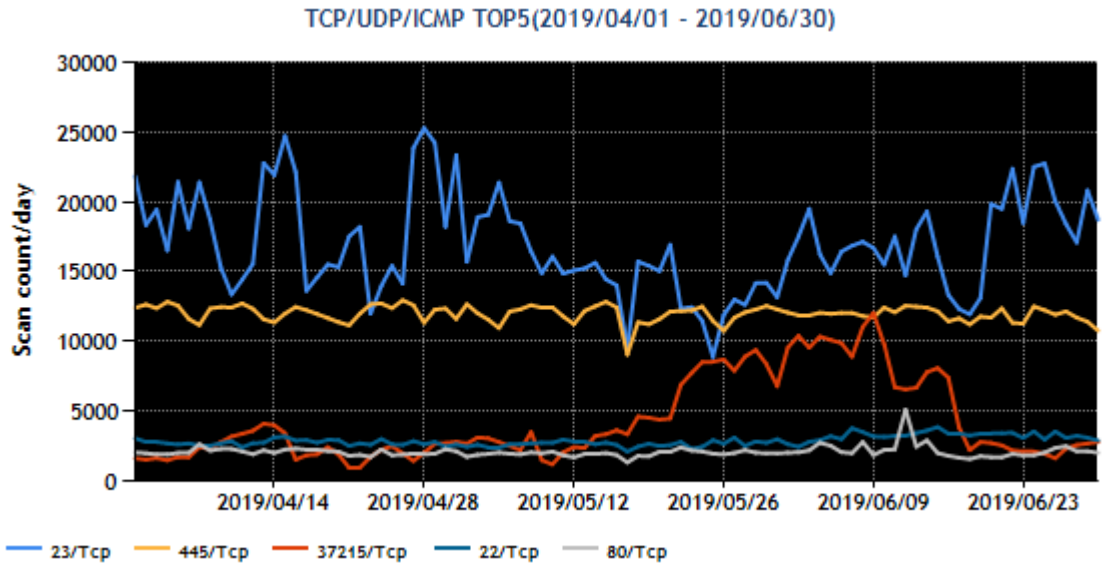
本四半期に国内で観測されたパケットの宛先ポート番号をパケットが多かった順に並べるとトップ 5 は［表 1］に示すとおりでした。

［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	23/TCP (telnet)	1
2	445/TCP (microsoft-ds)	2
3	37215/TCP	TOP10 外
4	22/TCP (ssh)	5
5	80/Tcp(http)	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。



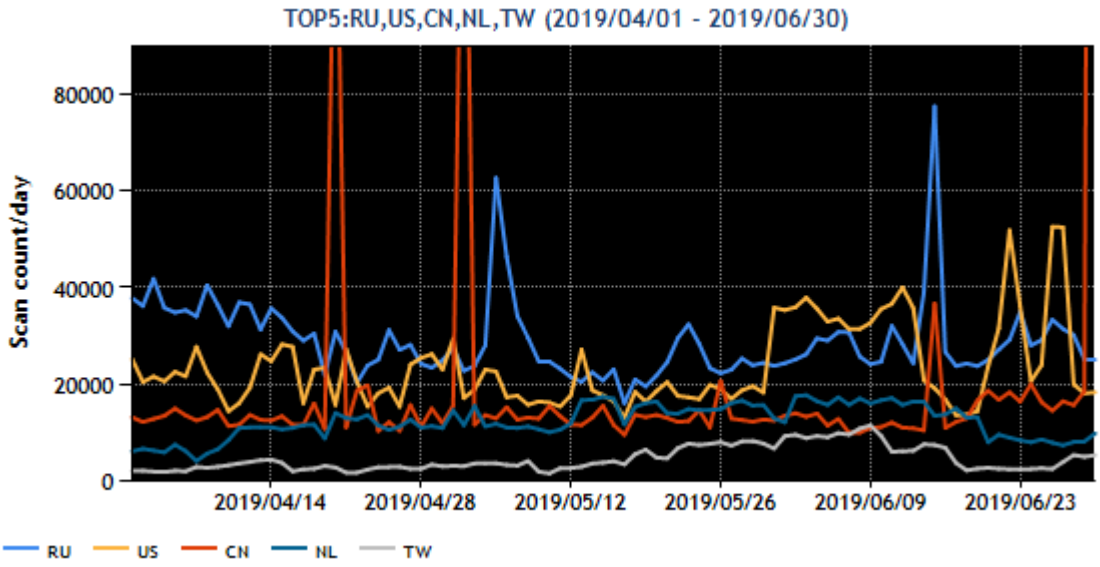
［図 1：2019 年 4～6 月の宛先ポート番号別パケット観測数トップ 5 の推移］

本四半期の期間中ほぼ一定数の 445/TCP 宛のパケットが観測され、その数が一時的に 23/TCP 宛のパケットを上回る期間もありました。37215/TCP 宛のパケットは、5 月 14 日頃から約 1 か月の間観測数が増加し、順位が 3 位に上がりました。約 7 割のパケットは送信元地域が台湾でした。当該期間、複数の機器の脆弱性に対して攻撃を行う Mirai 亜種が活動していたとの情報が公開されており、その中には CVE-2017-17215 が攻撃対象として含まれていました。このマルウエアの活動によって 37215/TCP 宛のパケットが増加した可能性も考えられます。
続いて、送信元の地域ごとの内訳を調べると、特定の 3 地域に著しく偏っていました。本現象については、2.1 節 「Windows 環境とみられる送信元からのパケット数の増加」で述べます。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	ロシア	1
2	米国	2
3	中国	3
4	オランダ	4
5	台湾	TOP10 外

［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。



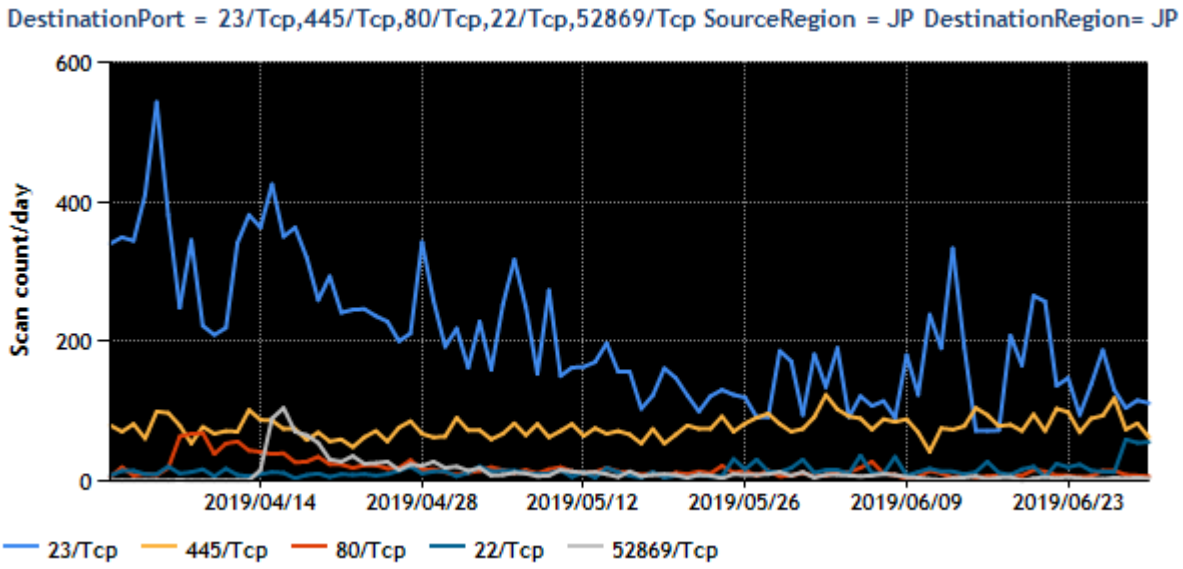
［図 2：2019 年 4～6 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

観測パケット数の送信元地域による内訳では、台湾が 5 月 12 日頃より増加しました。このため順位が変動しました。台湾地域からのパケットは 37215/TCP 宛が最も多く、台湾を送信元とするパケットの約 7 割を占めました。その他の地域については、一時的な増減がありしたが、通期の順位に変化を及ぼすほどではありません。

2. 注目された現象

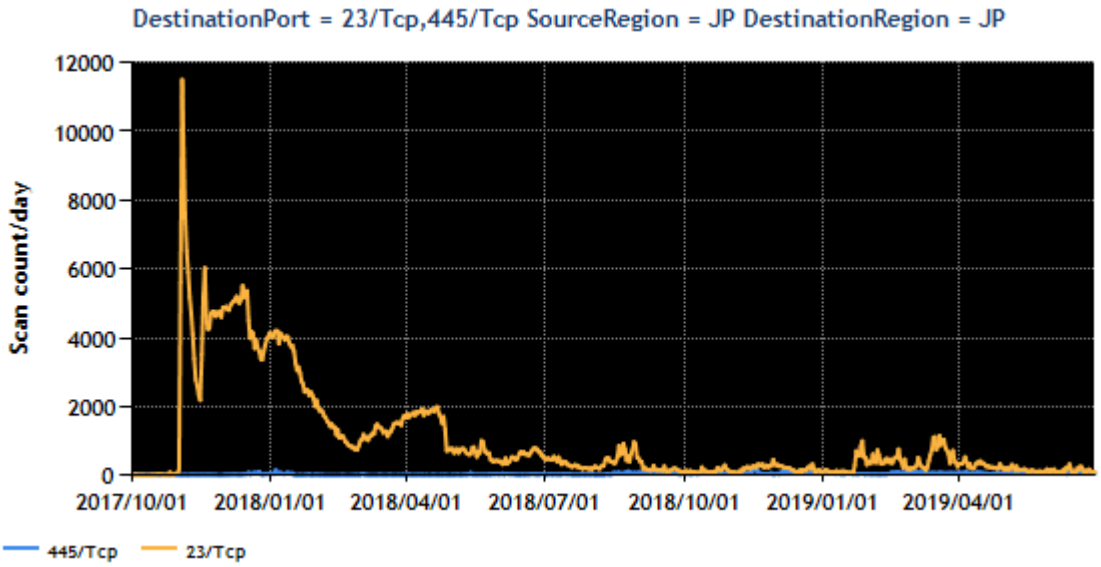
2.1. 日本から送信されたパケットの動向

日本を送信元とした宛先ポート番号別パケット観測数の 2019 年 4 月からの推移は［図 3］のとおりです。



［図 3：日本を送信元とした宛先ポート番号別パケット観測数トップ 5］

2017 年 11 月以降［図 4］、日本を送信元としたパケットは継続的に 23/TCP 宛が最も多く、その大部分は Mirai およびその亜種に感染した機器によるものでしたが、その後に製品ベンダーや ISP 等が対策実施を呼びかけ、ユーザによるアップデートや機器の交換等の対策が進んで、23/TCP 宛のパケットが減少してきました。これに替わり本四半期は、445/TCP 宛のパケットが少しずつ増加し、これが一時的には上回る時間帯も出てきました。

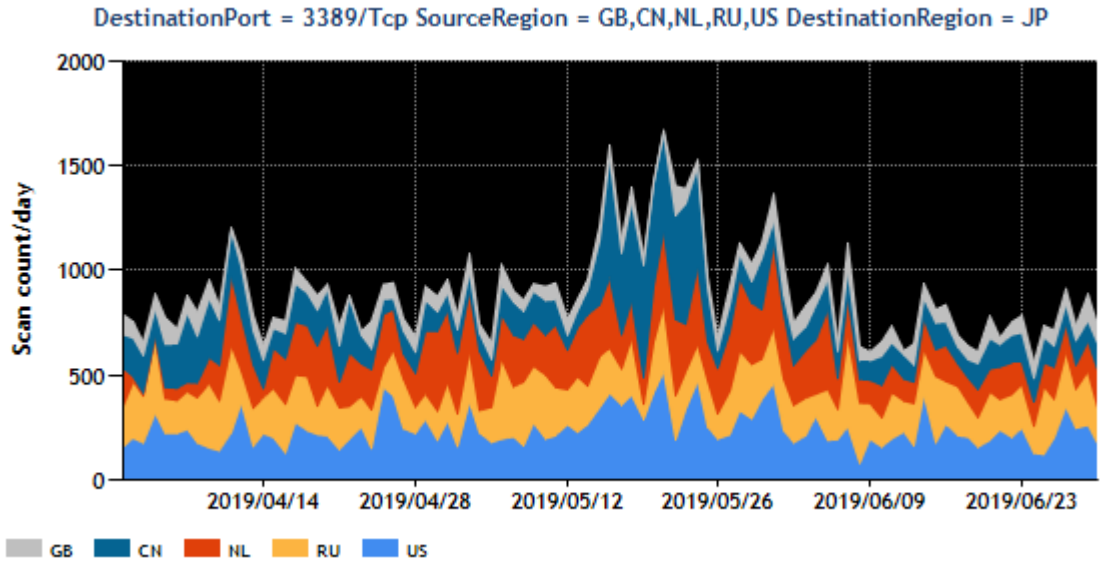


［図 4：23/TCP と 445/TCP 宛のパケットの長期間の推移］

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ある特徴があります。送信元の一部を確認したところ、古いバージョンを含む複数の Windows OS を確認できましたが、特定のバージョンやマシンの利用用途に偏っていると言った特徴は見られませんでした。445/TCP のポートを Windows では様々な用途で使用しています。このポートを通じて広く行われた攻撃事例を紐解くと、サーバ上で設定されている弱いアカウントのパスワード認証を突破し、システム上でマルウエアを実行させ感染させる手口や、Windows の既知の脆弱性を悪用することでサーバにマルウエアを感染させる手口が思い起こされます。その一つにマルウエア Wannacry があり、Wannacry が送信する TCP パケットのウインドウサイズの値には、今回観測されているものと同じ特徴があります。こうした状況から、今回の観測したパケットが、マルウエアに感染した Windows サーバからの感染範囲を拡大するためのものかと推測しています。なお、IP アドレスの管理者に連絡等を行っていますが、現時点ではパケット数の著しい減少はみられません。

2.2. 3389/TCP 宛のパケットの動向

本四半期の宛先ポート番号トップ 5 には入っていませんが、2019 年 5 月 14 日頃から約 10 日間 3389/TCP 宛のパケットの増加を観測しています。[図 5]に示した地域別の積上げグラフに見られるように、主な送信元は中国、米国、オランダ等です。



[図 5：Port3389/TCP 観測パケット数の主な送信元地域ごとの推移]

これらのパケット増加は、マイクロソフト社の Remote Desktop Service (CVE-2019-0708)の脆弱性に関する情報の公開(*2)の影響と考えられます。本脆弱性情報の公開直後からの約 2 週間パケット観測数が増加しました。
本脆弱性は、すでにサポートが終了した Windows XP や Windows Server 2003 も影響を受け、それらの OS に対してもマイクロソフト社から異例のセキュリティ更新プログラムが公開されています。

またマルウエア作成に使用される可能性が高いとして、他の機関も注意を呼び掛けています。
2020 年 1 月 14 日には、Windows Server 2008 / Windows Server 2008 R2 のサポートが終了します。
2.1 で述べた件もありますので、身の回りで稼働している機器の Windows がサポート対象となっているバージョンを使用しているか、セキュリティ更新が適切に実施されているか、不要なポートを開けたままにしていないか、適切な強度のパスワードを使用しているか等を確認してみることをお勧めします。

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) CVE-2019-0708 | リモート デスクトップ サービスのリモートでコードが実行される脆弱性
https://portal.msrc.microsoft.com/ja-JP/security-guidance/advisory/CVE-2019-0708

本活動は、経済産業省より委託を受け、「平成３１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。