JPCERT/CC インターネット定点観測レポート

2019 年 1 月 1 日 ～ 2019 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

2019 年 4 月 11 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。

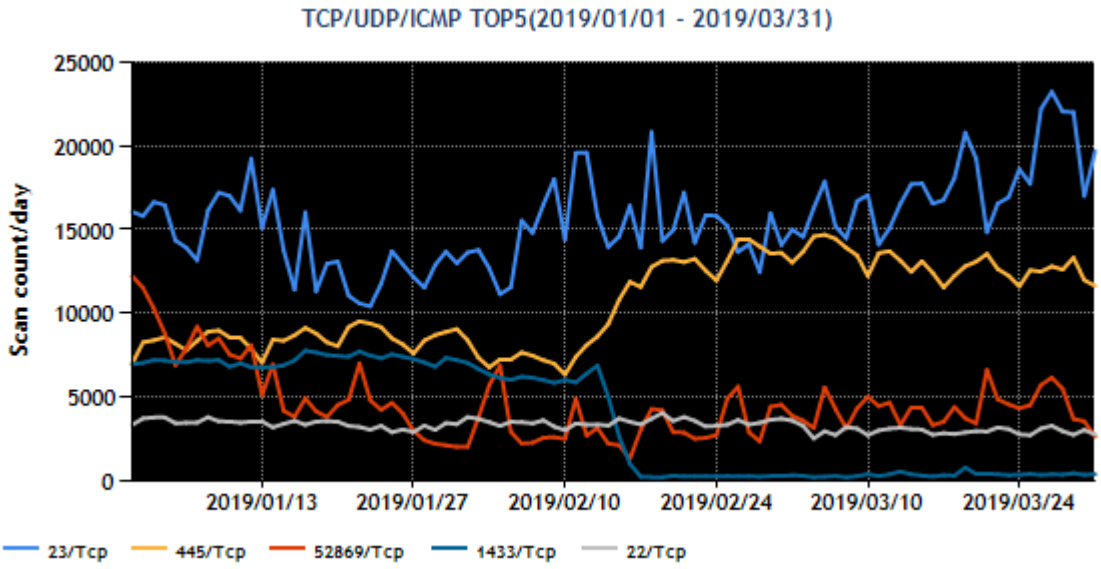
本四半期に国内で観測されたパケットの宛先ポート番号をパケットが多かった順に並べるとトップ 5 は［表 1］に示すとおりでした。

［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	52869/TCP	6
4	1433/TCP(ms-sql)	3
5	22/TCP (ssh)	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。



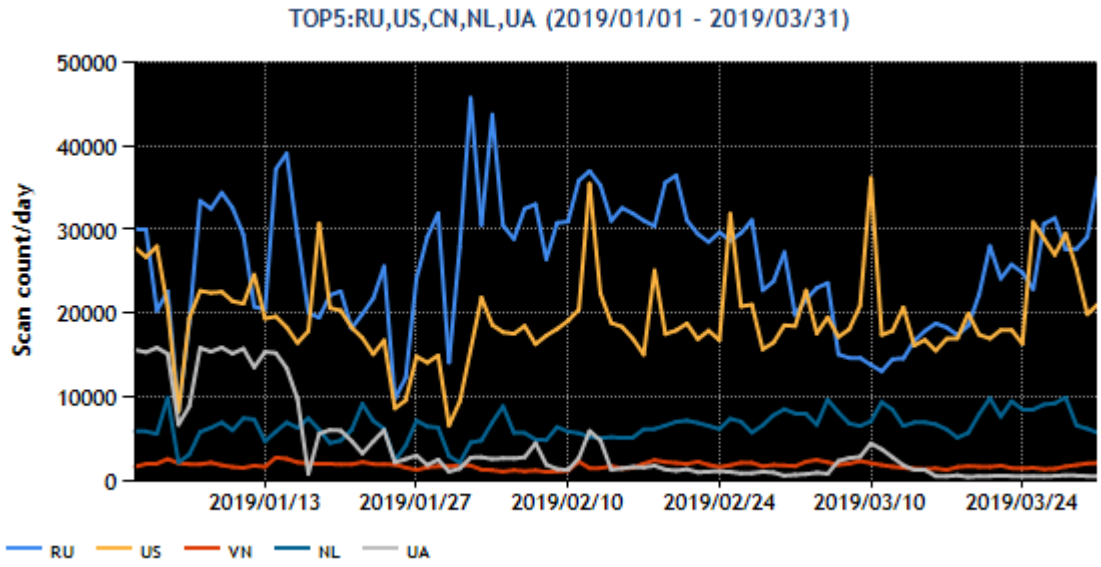
［図 1：2019 年 1～3 月の宛先ポート番号別パケット観測数トップ 5 の推移］

445/TCP 宛のパケットが、2 月 10 日頃から増加しています。また、1433/TCP 宛のパケットは、2 月 15 日頃から急減しました。52869/TCP 宛のパケットは、順位が 3 位に上がりました。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	5
5	ウクライナ	4

［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。



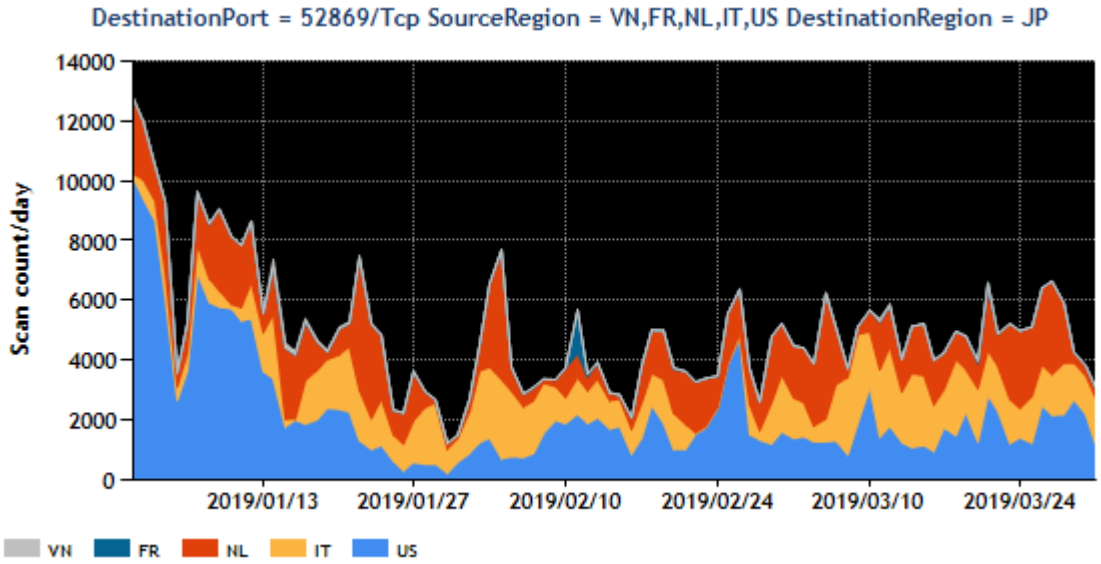
［図 2：2019 年 1～3 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

送信元地域では、ウクライナからのパケットが 1 月 19 日頃より減少し、オランダと順位が入れ替わりました、その地の地域では一時的な増減はありますが、順位に変化はありません。

2. 注目された現象

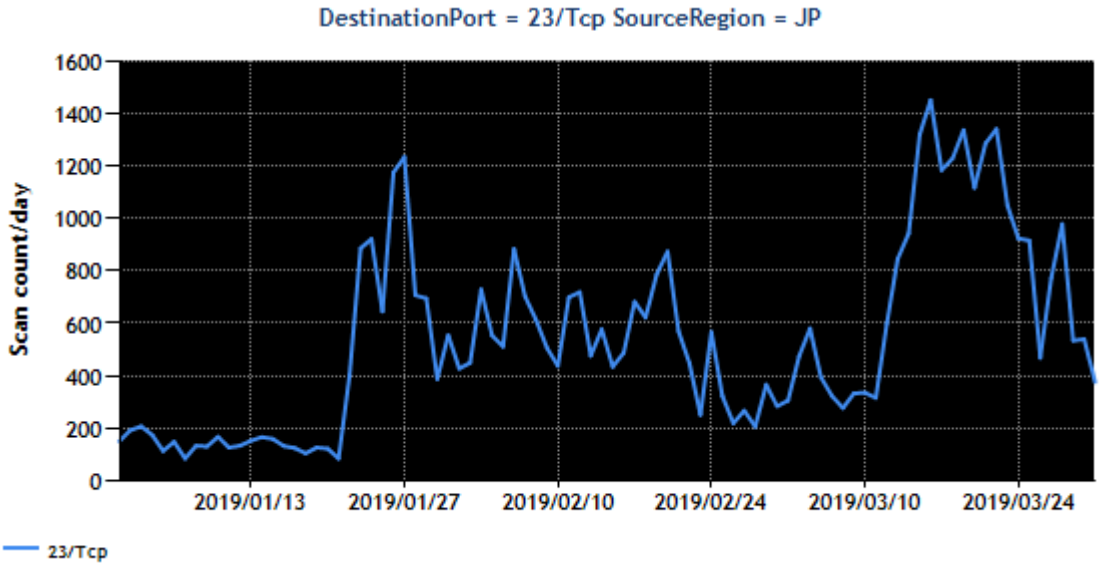
2.1. 52869/TCP 宛のパケットの動向

2019 年 1 月から 52869/TCP 宛のパケットを観測(*2)しています。主な送信元はアメリカ、イタリア、オランダです、地域別の積み上げグラフを［図 3］に示します。



［図 3：Port52869/TCP 観測パケット数の主な送信元地域ごとの推移］

これらのパケットの背景には、Realtek 社製 SDK Miniigd サービスの既知の脆弱性(CVE-2014-8361)[*3]が関連していることが調査の結果わかっています。同 SDK を使用して作られたルータは、脆弱性の影響を受けるためインターネット経由で攻撃を受ける可能性があります。日本国内にも当該脆弱性の影響を受ける機器がまだ数多く存在しています。この攻撃は、一旦感染させることに成功しても、その効果がルータの再起動で失われるため、攻撃を繰り返して再感染させているようで、そのために多くの攻撃パケットが観測されていると考えています。
また、1 月下旬からは、日本国内の IP アドレスから 23/TCP 宛のパケットが増加[*4]しています。[図 4]このパケットは、Mirai 亜種がもつ特徴がみられます。



[図 4：日本を送信元とした Port23/TCP 観測パケット数推移]

送信元の IP アドレスの一部を調査したところ、国内ベンダー製のブロードバンド・ルータが送信元になっており、上述の SDK の脆弱性 (CVE-2014-8361) への対策済みファームウエアを使用していないことが確認できました。
JPCERT/CC では、マルウエアに感染している脆弱なルータの利用者への対応として、順次当該 IP アドレスの管理者を通じて連絡し、対策をお願いしています。

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) 平成 31 年 1 月期観測資料
https://www.npa.go.jp/cyberpolice/important/2019/201903282.html

(3) インターネット定点観測レポート(2017 年 10～12 月)
http://www.jpcert.or.jp/tsubame/report/report201710-12.html#2.1

(4) NICTER 解析チーム（試験運用中）
https://twitter.com/nicter_jp/status/1102834623405416448

本活動は、経済産業省より委託を受け、「平成 30 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。