JPCERT-TBM-2019-01
発行日 : 2019-1-16

# JPCERT/CC インターネット定点観測レポート
# [2018 年 10 月 1 日～12 月 31 日]

## 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。

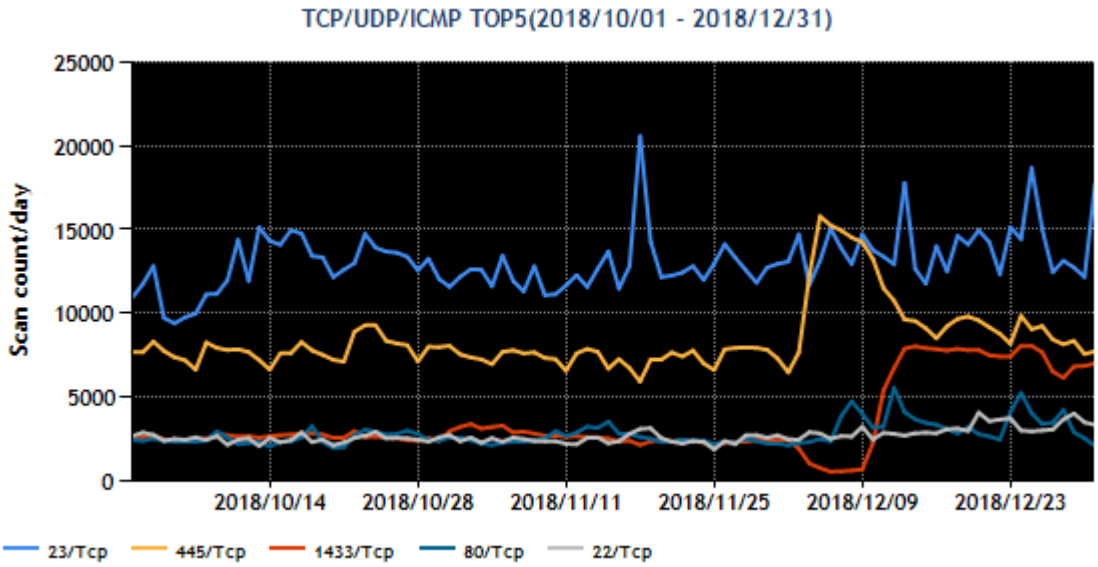
本四半期に国内で観測されたパケットの宛先ポート番号をパケットが多かった順に並べるとトップ 5 は［表 1］に示すとおりでした。

［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 | 1433/TCP (ms-sql) | 6 |
| 4 | 80/TCP(http) | 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。



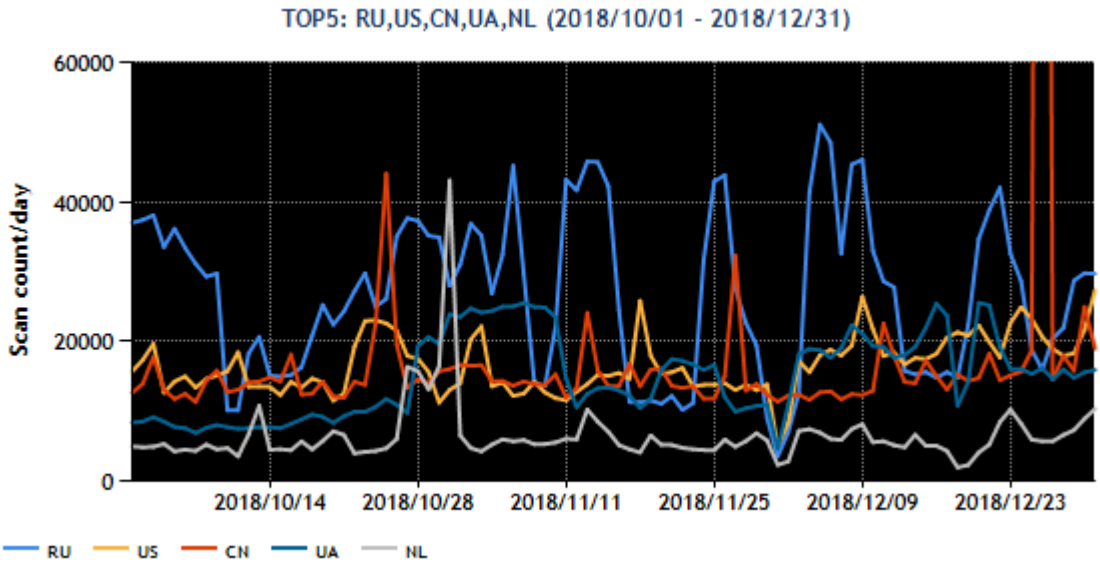

［図 1：2018 年 10～12 月の宛先ポート番号別パケット観測数トップ 5 の推移］

445/TCP 宛のパケットが、12 月 3 日頃に急増しました。また、1433/TCP 宛のパケットが、12 月 10 日頃に急増しています。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 | 2 |
| 2 | 米国 | 3 |
| 3 | 中国 | 1 |
| 4 | ウクライナ | 5 |
| 5 | オランダ | 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。



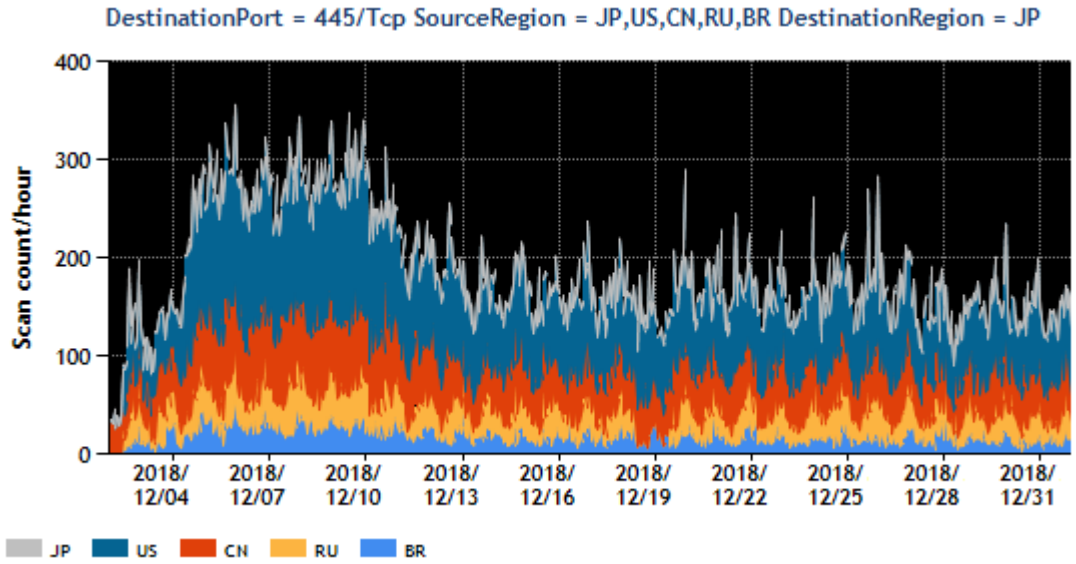

［図 2：2018 年 10～12 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

このように送信元地域に着目すると、前四半期の 8 月 20 日よりウクライナからのパケット数が増加した状態が今期も続いています。これに対して、中国からのパケットが他の地域からのものよりも多く観測された時期はごく短期だけにとどまり、順位が第 3 位まで後退しました。

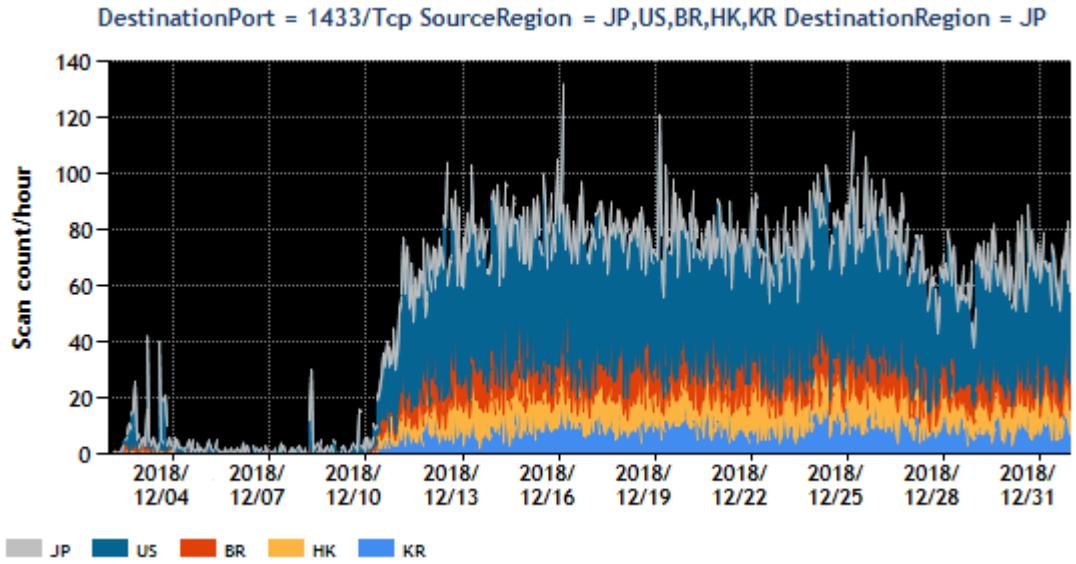
## 2. 注目された現象

### 2.1. Windows 環境とみられる送信元からのパケット

2018 年 12 月 3 日頃より、Port445/TCP 宛のパケットが多い状態が続いています［図 3］。また、12 月 10 日頃からは、Port1433/TCP 宛のパケットも多くなっています［図 4］。パケットには送信元 IP アドレスが国内のものだけでなく国外のものもあり、いずれもパケット数が以前と比べて多くなっています。また、この現象は日本に届いたパケットだけでなくほかの地域に届いたパケットでも観測されています。




［図 3：Port445/TCP 観測パケット数の主な送信元地域ごとの推移］

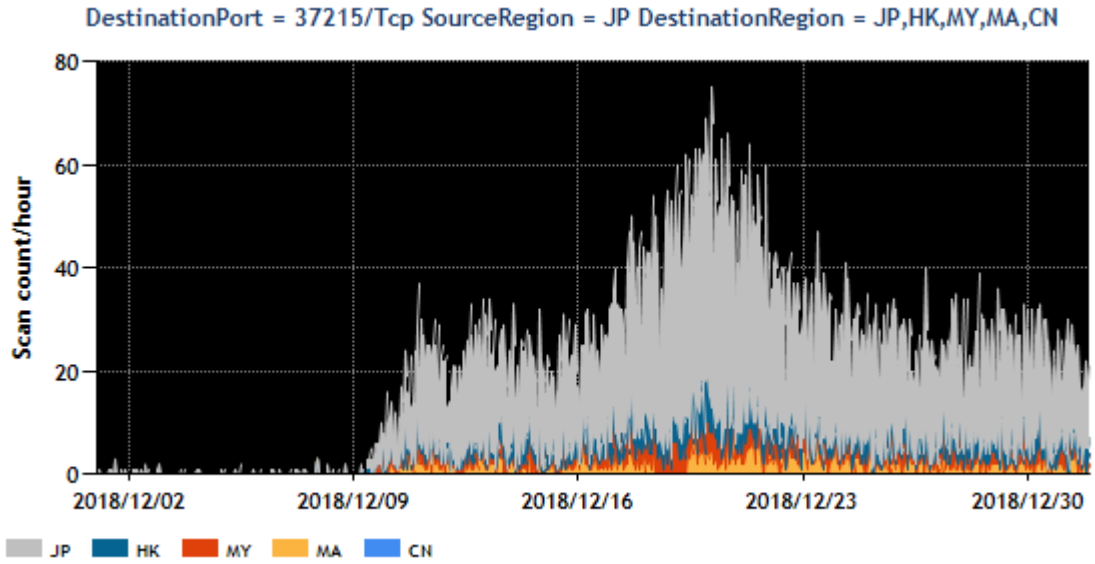



［図 4：Port1433/TCP 観測パケット数の主な送信元地域ごとの推移］

調査したところ、この 2 つのポートへのパケットの送信元となっているホストの多くで IIS や SMB が動作しており Windows 環境であろうと推測されました。Windows のバージョンは 2003 のものもありましたが、2008 や 2012 等の新しい OS も存在し、SMB のポートは空いているものも閉じられているものも見られ、共通した特徴は確認できませんでした。これらのホストが感染してパケットを送信しているマルウエアが何なのかについてはまだ分かっていません。
JPCERT/CC では、これらのパケットのうち、日本国内から発信され発信元が企業等とみられるものについて、当該 IP アドレスの管理者全てに連絡を行って本件に関する情報を収集しています。

### 2.2. 日本国内からの 37215/TCP 宛のパケット数の増加

2018 年 12 月 9 日頃より、日本国内を送信元とした Port37215/TCP 宛のパケットが増加(*2)しています［図 5］。同様のパケットは、海外のセンサーでも広く観測されています。パケットの送信元について調査を行ったところ、Realtek 社製の SDK の脆弱性 (CVE-2014-8361) (*3)の影響を受けた国内ベンダー製のブロードバンド・ルータであることが確認できました。それらのルータは複数の ISP 等に割り当てられた IP アドレスを使用していました。脆弱性の対策が放置されていて、Mirai 亜種に感染したルータと推測されます。マルウエアの影響を受けている脆弱なルータの利用者に対策をおこなっていただくため、順次当該 IP アドレスの管理者に JPCERT/CC から連絡を行っています。




［図 5：Port37215/TCP 観測パケット数の主な送信元地域ごとの推移］

## 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) NICTER 解析チーム（試験運用中）
https://twitter.com/nicter_jp/status/1072774530202972160

(3) 【ハニーポットで気になった】52869/tcp および 8081/tcp 宛を狙った攻撃ってどんなもの？
https://sec-chick.hatenablog.com/entry/2019/01/05/145542

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。