JPCERT-TBM-2018-04
発行日 ：2018-10-18

JPCERT/CC インターネット定点観測レポート
[2018 年 7 月 1 日～9 月 30 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。

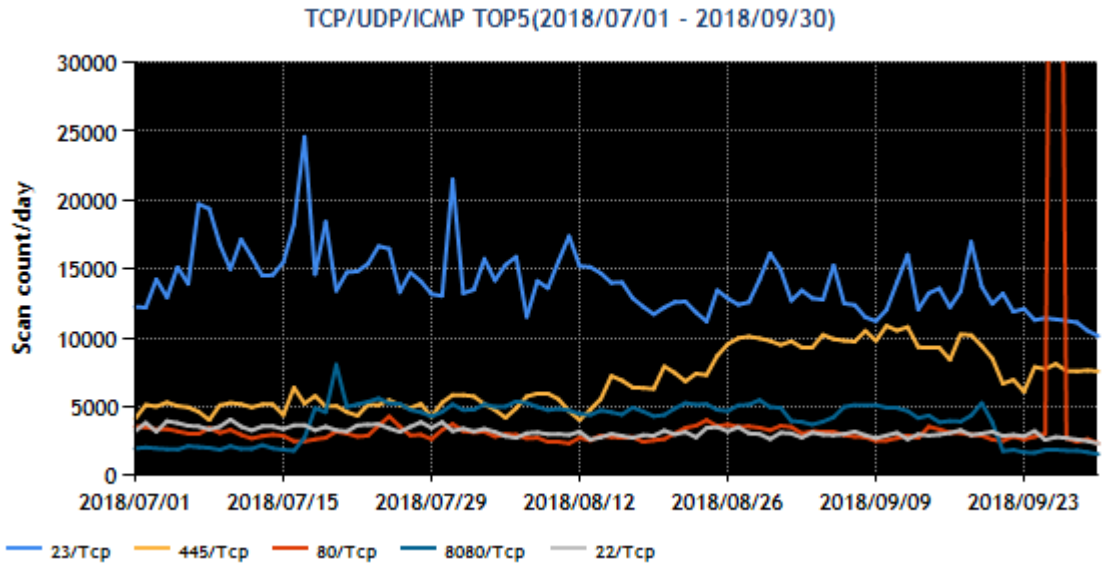
本四半期に国内で観測されたパケットの宛先ポート番号をパケットが多かった順に並べるとトップ 5 は［表 1］に示すとおりでした。

［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	80/TCP(http)	3
4	8080/TCP	6
5	22/TCP (ssh)	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］に示した宛先ポート番号の各パケット観測数の推移を［図 1］に示します。



［図 1：2018 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］

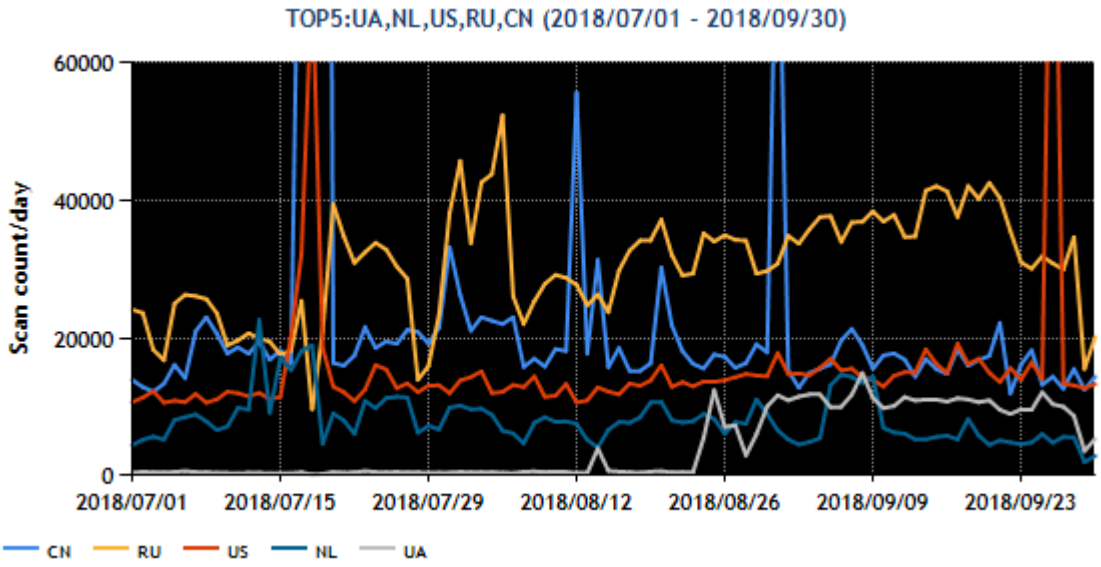
445/TCP 宛のパケットが、8 月 12 日以降増加傾向にあります。本現象については、「2.1 Port445/TCP 宛のパケット数の増加」の節で述べます。
また、8080/TCP を含む複数のポートに対してパケットが増加したことが読み取れますが、これは一部のマルウエアが探索するポートを変更した影響であろうと考えられます。

同様に、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	中国	2
2	ロシア	3
3	米国	1
4	オランダ	5
5	ウクライナ	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。



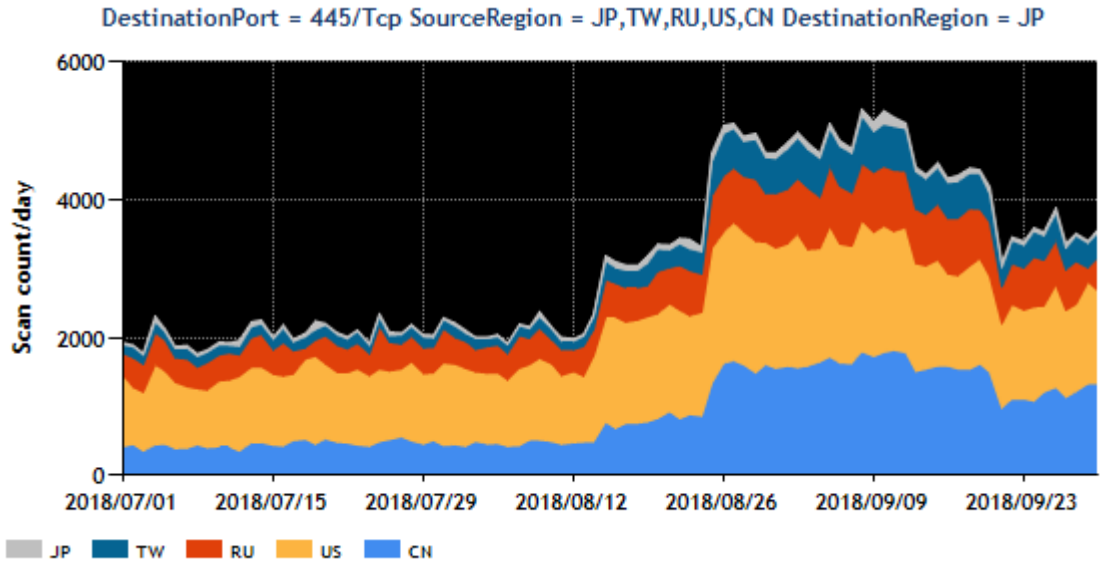
［図 2：2018 年 7～9 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

次に送信元地域に着目すると、ウクライナからのパケットが 8 月 20 日頃から増加傾向にあります。送信元となっている機器は同じ番号のポートが開いていました。当該地域で広く使用されている機器がマルウエアに感染して、これらのパケットを送信していると考えられます。

2. 注目された現象

2.1. Port445/TCP 宛のパケット数の増加

2018 年 8 月 12 日頃より、Port445/TCP 宛のパケットが増加(*2)しています［図 3］。パケットの送信元 IP アドレスには国内のものも国外のものもあり、いずれもパケット数が以前と比べて増えています。この現象は日本だけでなくほかの地域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］

Port445/TCP 宛のパケットは、2017 年 5 月以降 WannaCry 等の探索活動に伴うものが観測されました(*3)が、8 月 12 日以降はそれとは特徴が異なるパケットが含まれるようになりました。この特徴を持つパケットの送信元となっている国内外の IP アドレスについて調査を行ったところ、8 割以上で Windows2003 が稼働しているホストでしたが、それ以外にも Windows2008R2 等のバージョンが確認されました。Windows2003 だけに関連した問題ではないと考えられます。

日本国内から発信されたパケットのうち、発信元が企業等とみられたものについて、当該 IP アドレスの管理者全てに連絡を行いました。一部の管理者からは、アンチウイルスソフトでマルウエアが発見されたという回答をいただきましたが、検知結果の詳細やマルウエアの検体は得られていません。JPCERT/CC では本件に関する情報収集を継続して行っています。

今回確認された多くの場合では Windows2003 が OS として使用されていました。インターネットに公開するサーバには、メーカーによる脆弱性への対応(*4)が行われている OS を使用してください。

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 30 年 8 月期観測資料
https://www.npa.go.jp/cyberpolice/detect/pdf/20180928_1_toukei.pdf

(3) インターネット定点観測レポート(2017 年 7～9 月)
https://www.jpcert.or.jp/tsubame/report/report201707-09.html#2.2

(4) Windows Server 2003 の拡張サポートは 2015 年 7 月 14 日に終了しました。
https://www.microsoft.com/ja-jp/cloud-platform/windows-server-2003

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。