JPCERT CC®

Japan Computer Emergency Response Team Coordination Center

JPCERT-TBM-2017-03
発行日 ： 2017-08-03

JPCERT/CC インターネット定点観測レポート
[2017 年 4 月 1 日～6 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、本四半期に国内に設置されたセンサーで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。

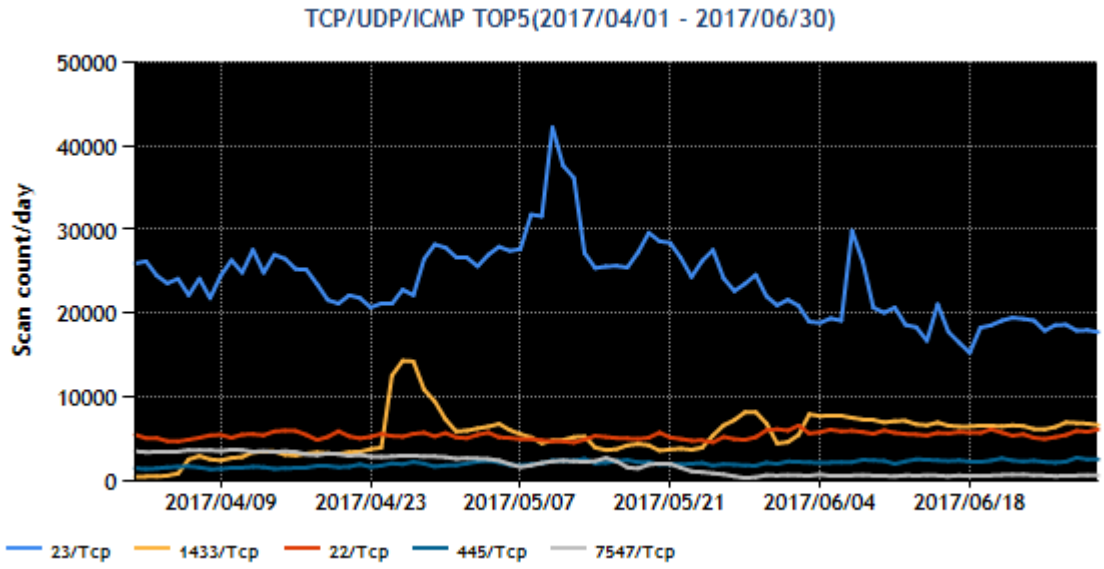
宛先ポート番号別パケット観測数のトップ 5 を［表 1］に示します。

［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	1433/TCP(ms-sql-s)	トップ 10 外
3	22/TCP (ssh)	3
4	445/TCP(microsoft-ds)	トップ 10 外
5	7547/TCP(cwmp)	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。

図 1 は、期間中のトップ 5 の宛先ポート番号ごとのパケット観測数の推移を示しています。



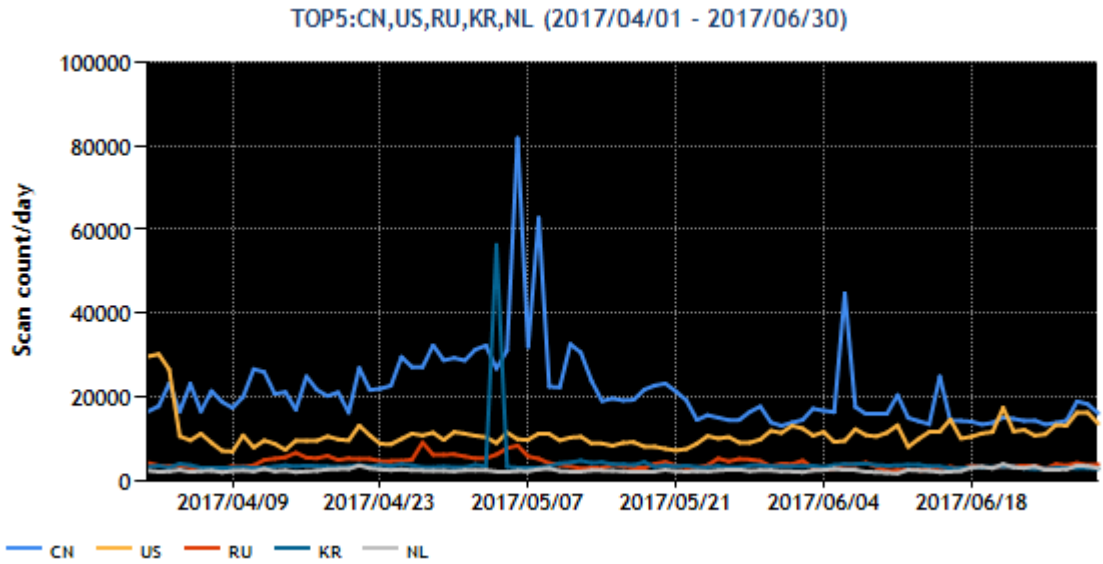
［図 1：2017 年 4～6 月の宛先ポート番号別パケット観測数トップ 5 の推移］

送信元地域のトップ 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	1
2	米国	2
3	ロシア	7
4	韓国	4
5	ブラジル	6

図 2 に期間中のトップ 5 のパケット送信元地域からのパケット観測数の推移を示します。



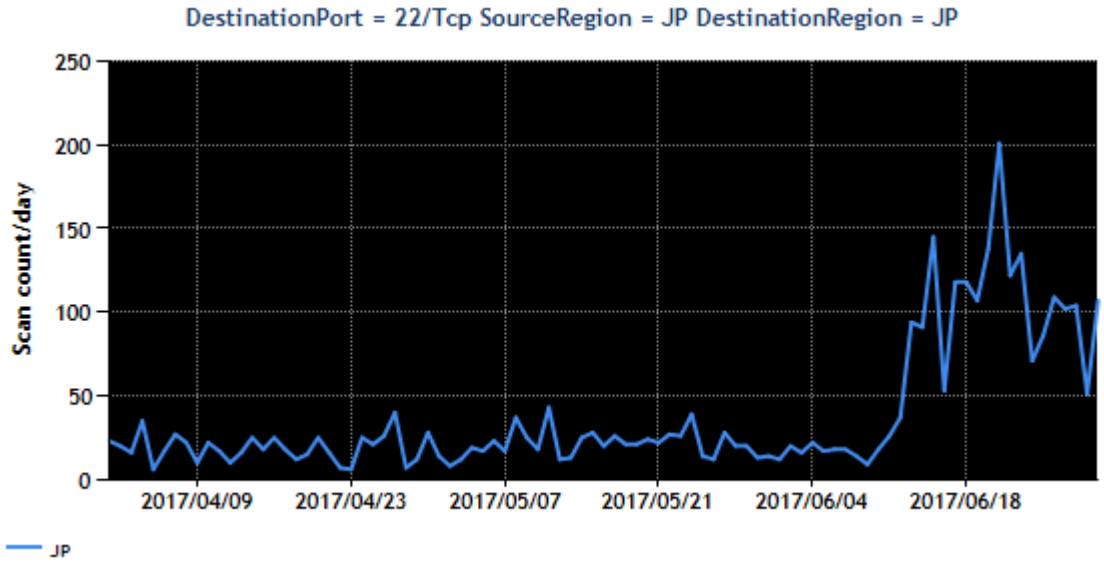
［図 2：2017 年 4～6 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

本四半期は、Windows の SQLServer と SMB サービスのリクエスト用 Port に対するパケットが多数観測されました。その他、前四半期もトップ 5 に入っていた、一部のベンダー製の Web カメラ、ルータ、NAS 等の機器が待ち受けている 22/TCP や 23/TCP 等のポートに対するパケットも継続して観測しています。その他に関しては、特筆すべき状況の変化は見られませんでした。

2. 注目された現象

2.1. Port22/TCP 宛のパケット数の増加

国内の IP アドレスから SSH サーバが使用する Port22/TCP に対するパケットが 2017 年 6 月 13 日頃より増加し、その後も増減はありますが継続して観測(*2)されています。（図 3）



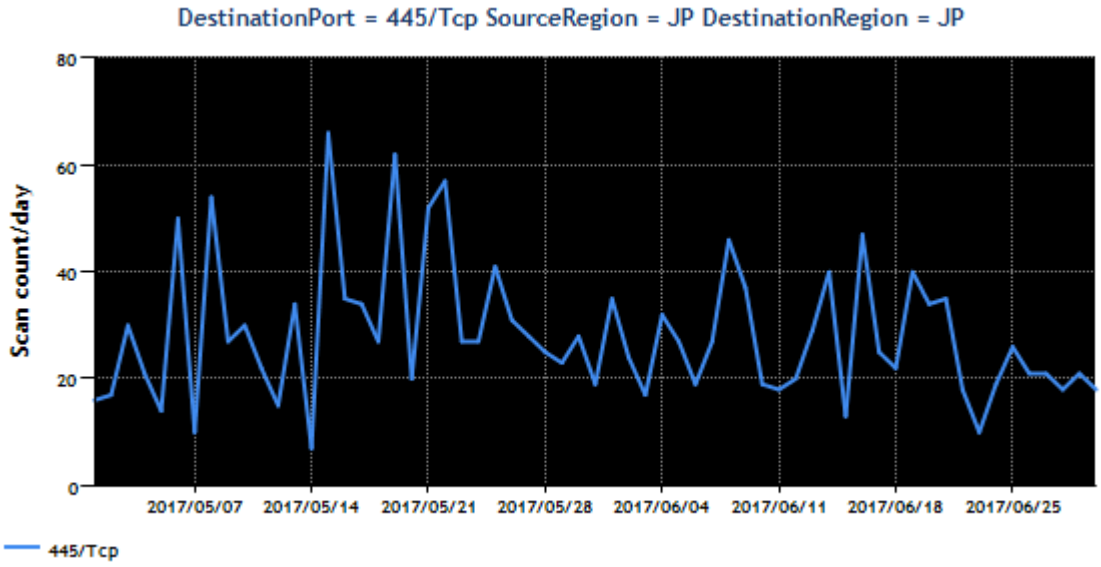
［図 3：Port22/TCP 宛のパケットの観測数の推移］

これらのパケットの多くは、国内の一部の移動体通信事業者や仮想移動体通信事業者と思われるネットワークから送信されています。一部の送信元 IP アドレスを調査してみると、組込みソフトウエアを搭載した専用機器が動作しているような挙動が観測できました。しかしながら、現時点では具体的な製品名や製造ベンダーは確認できておりません。

JPCERT/CC では、観測されたパケットのログ情報を通信事業者に報告し、送信元となっているユーザへの連絡をお願いできないか、協力を呼びかけています。

2.2. 国内からの 445/TCP 宛のパケット増加

5 月の上旬から、445/TCP に対するパケット数が増加しました。この時期に国内外で流行したランサムウエア WannaCry やその亜種は、マルウエアが動作し始めた際にほかの PC に感染拡大を試みる探索行為を行います。今回パケット数が増加したのは、マルウエア WannaCry の流行(*3 *4)の影響とみられます。



［図 4. Port445/TCP 宛のパケットの観測数の推移］

JPCERT/CC では、パケットの送信元がマルウエアに感染している可能性を疑い、IP アドレスの管理者に情報を提供して感染の有無の確認を求める活動を行っています。一部の管理者からは、マルウエアが検出された旨の返信をいただきました。

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) 国内からの 22/TCP ポートへのアクセスの増加
https://www.jpcert.or.jp/newsflash/2017070701.html
(3) ランサムウェア「WannaCry」に感染した PC からの感染活動とみられる 445/TCP ポート宛てアクセスの観測について
https://www.npa.go.jp/cyberpolice/important/2017/201705191.html
(4) ランサムウェア「WannaCry」の亜種に感染した PC からの感染活動とみられる 445/TCP ポート宛てアクセスの観測について
https://www.npa.go.jp/cyberpolice/important/2017/201706221.html

本活動は、経済産業省より委託を受け、「平成 29 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。