JPCERT CC®

Japan Computer Emergency Response Team Coordination Center

JPCERT-TBM-2017-04
発行日 : 2017-11-30

JPCERT/CC インターネット定点観測レポート
[2017 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、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。

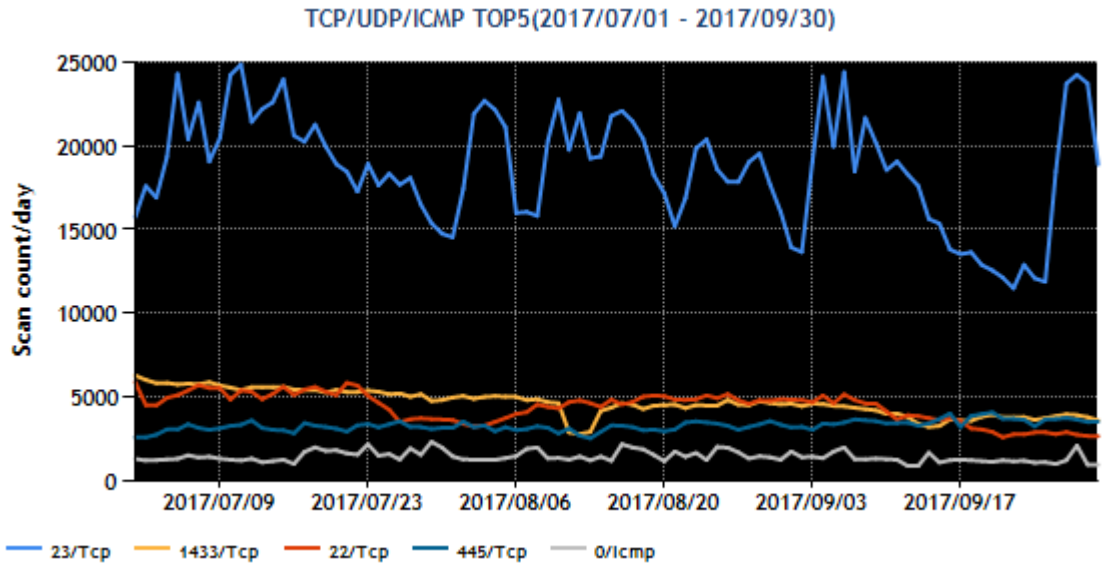
宛先ポート番号別パケット観測数のトップ 5 を［表 1］に示します。

［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)	2
3	22/TCP (ssh)	3
4	445/TCP(microsoft-ds)	4
5	Icmp	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。



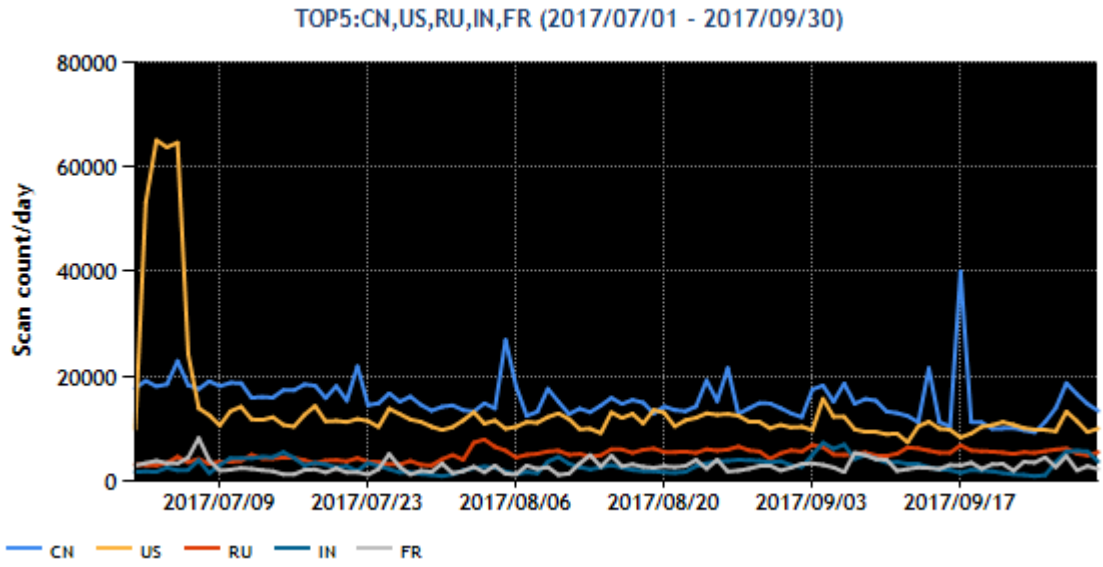
［図 1：2017 年 7～9 月の宛先ポート番号別パケット観測数トップ 5 の推移］

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	3
4	インド	7
5	フランス	9

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。



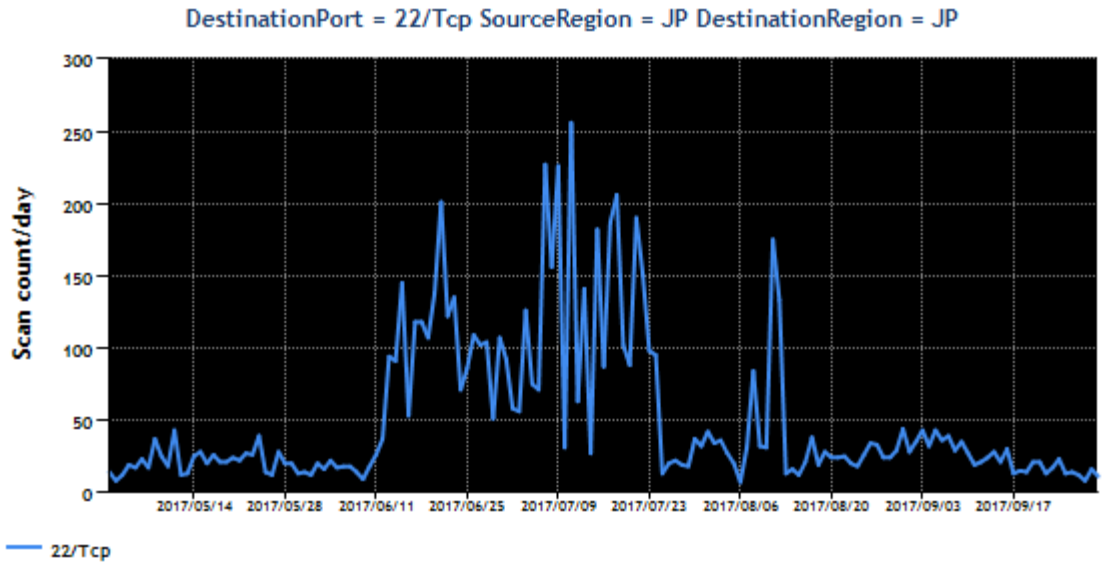
［図 2：2017 年 7～9 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

本四半期は、前四半期同様 Windows の SQLServer と SMB サービスのリクエスト受付用ポート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、脆弱な Web カメラ、ルータ、NAS 等の機器を狙ったとみられる 22/TCP や 23/TCP 等の宛先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

前回のインターネット定点観測レポート「2.1. Port22/TCP 宛のパケット数の増加」(*2)で、SSH サーバを狙ったとみられる Port22/TCP に対するパケットが 2017 年 6 月 13 日頃より一時的に増加し、その後増減を繰り返した後パケット数が減少したことを記載しましたが、減少後の水準ながら現在も継続して観測しています。(図 3)



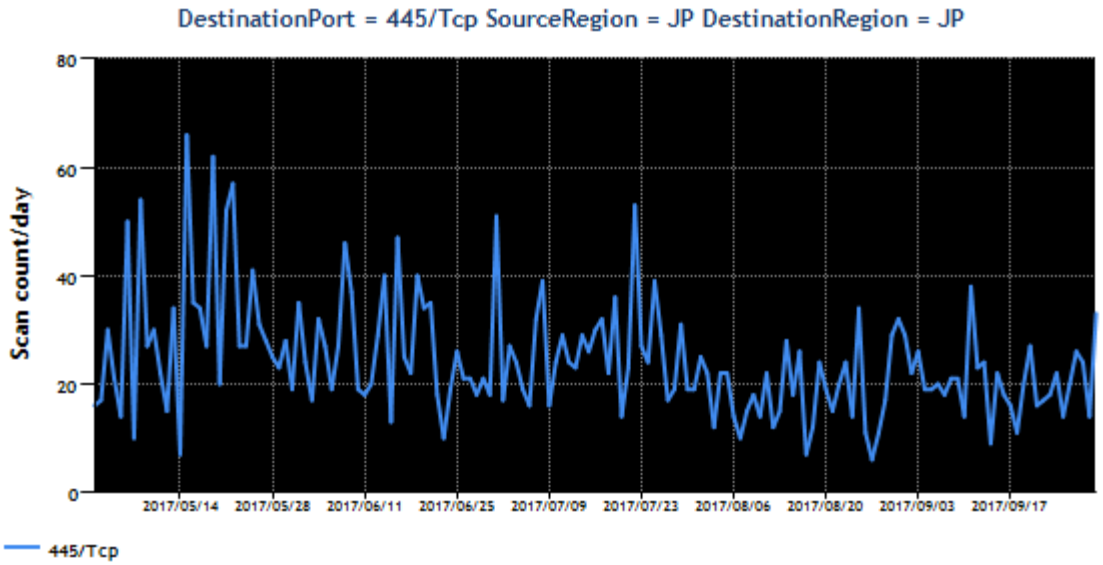
［図 3：Port22/TCP 宛のパケットの観測数の推移］

これらのパケットの多くは、日本で移動体通信サービスを提供する NTT ドコモや、仮想移動体通信サービスの OCN やぷららと推測されるネットワークから送信されていました。6 月から継続して観測した TCP パケットのパラメータの一部に特徴(*3)があったことから、パケットを送信している機器が特定のマルウエアに感染していると推測し、送信元の IP アドレスを管理する通信事業者に対して連絡を行う等の対応を行いつつ、詳細な調査を進めました。具体的には、他の研究機関よりハニーポットのデータを借用し、攻撃者が試している複数のログインアカウント情報をリスト化し、それを使って日本で高いシェアをもつ複数のネットワーク機器にログインを試みたところ、ログインして任意のコードを実行できることを確認しました。遠隔から第三者が任意のコマンドを実行できてしまう脆弱性として本件の届け出を行い、関係機関による調整を経て、製品開発者による対策情報とともに 9 月 12 日に JVN(*4) 等で情報が公開されました。

6 月にパケットの増加がみられ、その後、7 月下旬には一度に減少しましたが、8 月の上旬には一時的な増加が見られました。その後はゆるやかな増減があったものの、JVN での情報公開を境に、パケットは減少しています。JPCERT/CC では、観測されたパケット情報を送信元の IP アドレスを管理する通信事業者に報告し、送信元となっているユーザに対応を呼びかけるよう依頼しています。

2.2. 国内からの 445/TCP 宛のパケットの観測状況について

5 月の上旬から、445/TCP に対するパケットを継続して観測しています。



［図 4. Port445/TCP 宛のパケットの観測数の推移］

JPCERT/CC では、これらのパケットが WannaCrypt（別名 WannaCry）等のマルウエアに感染した機器から送信されている可能性が高いと考え、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いました。その結果、一部の管理者からは WannaCrypt が検出された旨の返信をいただきました。

5 月上旬に国内外で広まったランサムウエア WannaCrypt やその亜種は、動作し始める際に他の PC に 445/TCP を使って感染拡大を試みる探索を行います。TSUBAME で観測されたのは、こうした探索のためのパケットです。WannaCrypt の場合には、感染した機器がキルスイッチへのアクセスを試み、アクセスに成功した場合には、活動を止め、他の PC を探索するためのパケットは送信しませんが、WannaCrypt の一部の亜種は、キルスイッチへのアクセスに成功しても、他の PC を感染させる活動を続けることが確認されています (*5)。それらの亜種は、ファイルの暗号化や脅迫画面の表示などをせず、ユーザは感染になかなか気付きません。

445/TCP 宛のパケットは継続して観測しているため、セキュリティ更新プログラムを適用していない脆弱な PC は攻撃を受ける恐れがあります。また日本国内からも新たにパケットの送信元となる PC が確認されています。セキュリティ対策が徹底されているか、また外部に 445/TCP 宛のパケットを送信していないか、ファイアウォールやルータ等のログを確認することをおすすめします。

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) インターネット定点観測レポート(2017 年 4～6 月)
https://www.jpcert.or.jp/tsubame/report/report201704-06.html

(3) Hajime, Mirai による通信の推移
https://sect.iij.ad.jp/d/2017/09/072602.html

(4) JVN#68922465 Wi-Fi STATION L-02F にバックドアの問題
https://jvn.jp/jp/JVN68922465/

(5) WannaCry まだ終わってなくない?
https://sect.iij.ad.jp/d/2017/09/192258.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。