電子署名者 : Japan Computer Emergency Response Team Coordination Center
DN : c=JP, st=Tokyo, l=Chiyoda-ku, email=office@jpcert.or.jp, o=Japan Computer Emergency Response Team Coordination Center, cn=Japan Computer Emergency Response Team Coordination Center
日付 : 2015.07.28 18:39:50 +09'00'

JPCERT-IA-2015-03
発行日 : 2015-07-29

JPCERT/CC インターネット定点観測レポート
[2015 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。なお、本レポートでは、本四半期に観測された日本宛のパケットを中心に分析した結果について述べます。

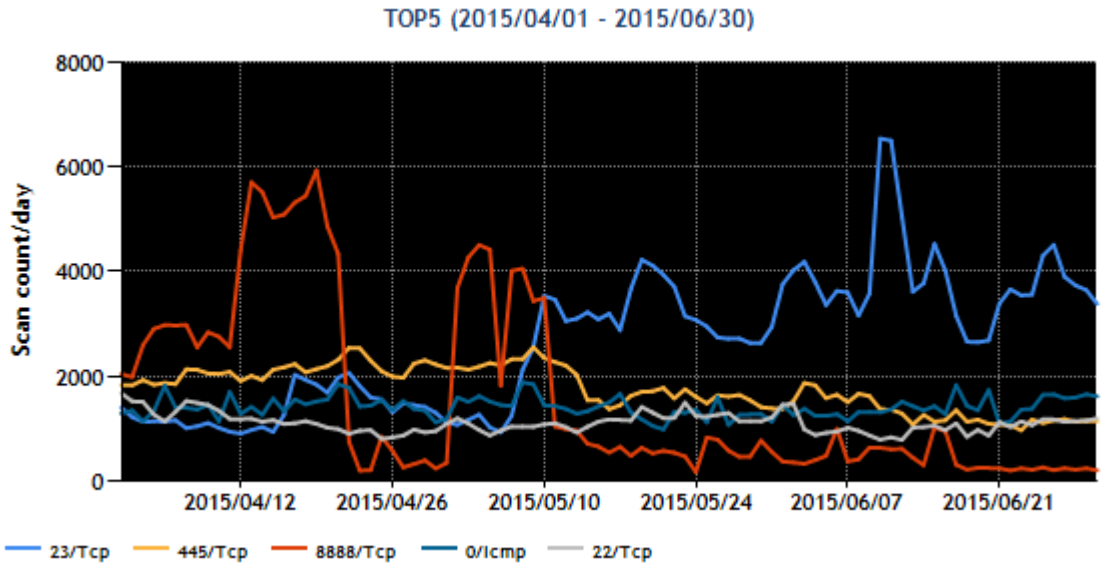
宛先ポート番号別パケット観測数のトップ 5 を [表 1]に示します。

[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	445/TCP (microsoft-ds)	4
3	8888/TCP	13
4	0/ICMP	2
5	22/TCP (ssh)	3

※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。



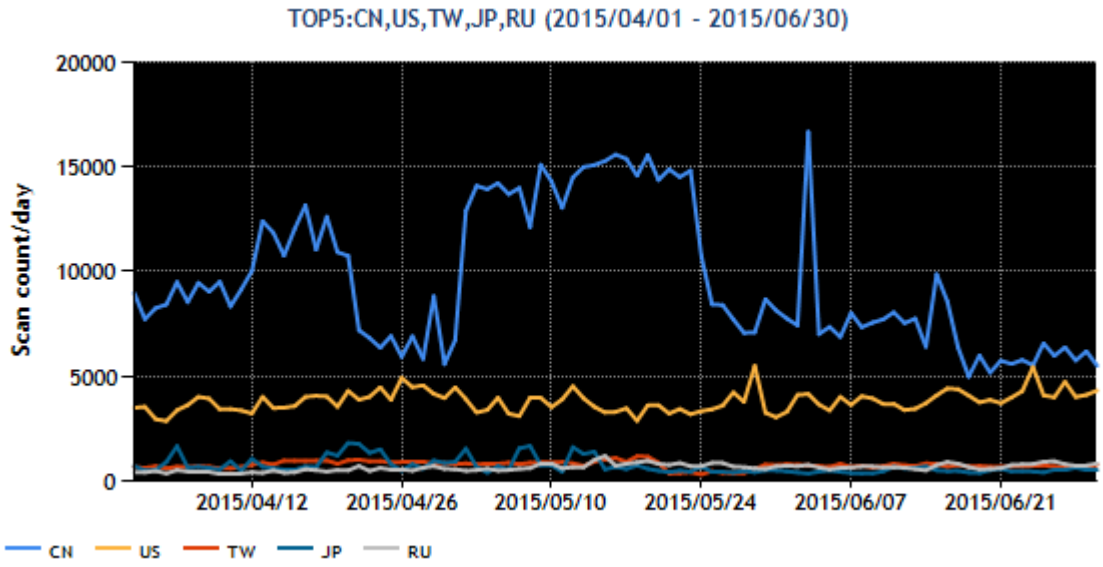
[図 1：2015 年 4~6 月の宛先ポート番号別パケット観測数トップ 5]

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	台湾	4
4	日本	3
5	ロシア	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。



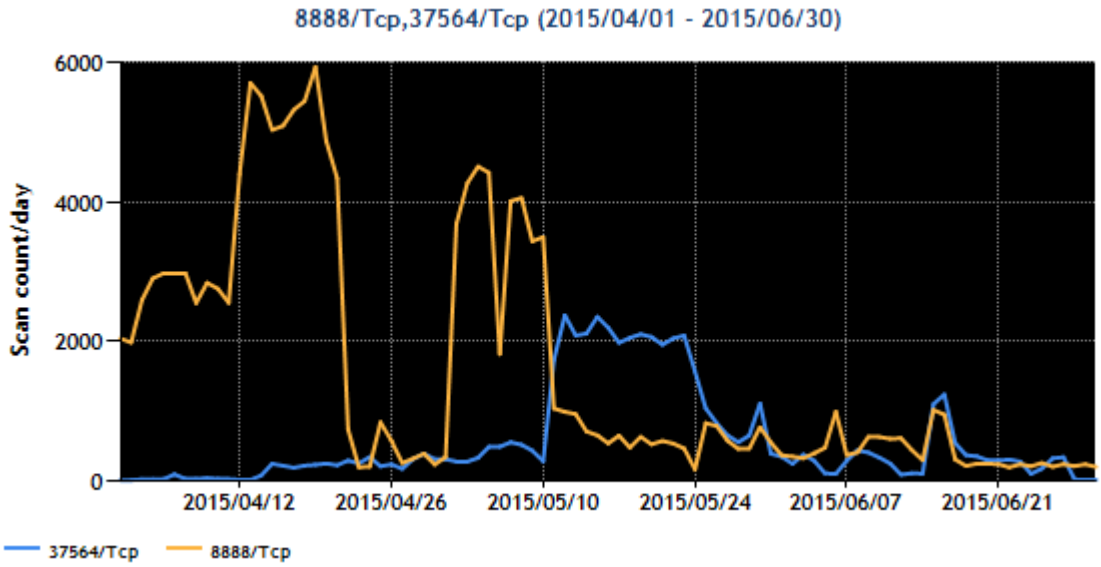
[図 2：2015 年 4~6 月の送信元地域別トップ 5 ごとのパケット観測数]

Telnet サーバを搭載したネットワーク機器を対象とする探索活動については、過去の定点観測レポートでも紹介しましたが、本四半期も 5 月 7 日頃から 23/TCP 宛のパケット数が再び増加しました。また、インターネット定点観測レポート(2015 年 1～3 月) [*2] で言及した 445/TCP 宛のパケットが 3 月中旬から 5 月中旬にかけて増加した結果、2 位に位置しています。
そのほか、4 月中旬から 8888/TCP 宛のパケットが増加しています。この増加の原因は、オープンプロキシサーバの探索活動の影響と思われ、2.1 で詳しく取りあげます。

2　注目された現象

2.1　オープンプロキシサーバの探索と推測されるパケットの増加

本四半期は、4 月上旬から 5 月中旬にかけて 8888/TCP、37564/TCP など複数のポート番号へのパケットが増加しました(図 3)。(*3) 8888/TCP 宛のパケットは、通期で第 1 位の 23/TCP 宛のパケットよりも多く観される日(or 週)が約 6 週間に渡って続いたほど増えたため、13 位から 3 位にランクインしました。

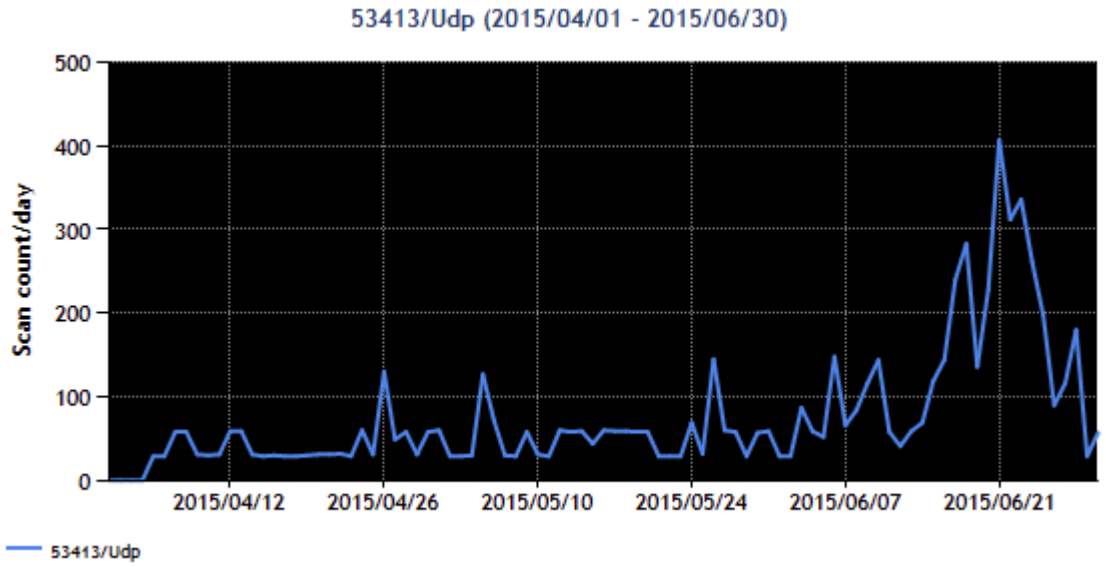


[図 3. 2015 年 4 月～6 月の 8888/TCP、37564/TCP 宛てのパケット観測数]

これらのポート番号宛の多量のパケットの発信目的を考察した時に最初に思い起こされるのが、オープンプロキシサーバのリストとして、IP アドレスとポート番号を掲載している海外の複数の Web サイトの存在です。これまでの TSUBAME の過去の観測では、何度となく通常サービスに使用されていないポート番号に対するパケットが急増するという事象がありました。今回、宛先ポート番号が 8888/TCP や 37564/TCP のパケットと同じ送信元 IP アドレスをもつパケットを探してみると、従来から知られているオープンプロキシサーバのポート番号宛のパケットが見つかるケースがあります。対応するオープンプロキシサーバのリストを調べると、8888/TCP などのポート番号の情報が新たにリストに追加されていて、このことからオープンプロキシサーバの探索を目的としたパケットであったことが高い確度で推測されます。これらのポート番号を標準的に用いるメジャーなプロキシサーバ―ソフトは知られておらず、何らかのパッケージ・ソフトウェア製品が内部的に稼働させているプロキシ―サーバが、不適切なネットワーク・アクセス制御のために、インターネットに露出していることが疑われます。いずれにせよ、こうしたポート番号に気づいたオープンプロキシサーバのリストの管理者が、探索ポートとして追加したことが、この種のパケットの観測数が一時的に増えた原因であろうと推測しています。

2.2　53413/UDP 宛のパケットの増加

2015 年 6 月 10 日頃から 2 週間ほど 53413/UDP 宛のパケットが増加しました (図 4) 。



[図 4. 2015 年 4 月～6 月の 53413/UDP 宛てのパケット観測数]

このポート番号は、日本で広く利用されている製品ではほとんど使用されていません。2014 年 8 月 27 日に公開されたトレンドマイクロ社のブログ記事によると、Netis/Netcore 社製のルータ製品には脆弱性があり、このポート番号に細工したパケットを送ることで、ルータが用意している任意のコマンドを遠隔の第三者がルータ上で実行できるとされています (*4)。この問題は、9 月 5 日までに製品ベンダがフォームウエアを更新し、解消されました。該当ポート番号にアクセスはできなくなったことをトレンドマイクロ社でも確認しています(*5)。

6 月中旬に増加したパケットは、この脆弱性を悪用して Bot に当該製品を感染させるものだったことが JPCERT/CC の調査で分かりました。その手口は、次のとおりです。

1. 攻撃者は、当該ルータの 53413/UDP に対し認証用パケット送信することで、認証を完了させる
2. 細工した 53413/UDP パケットを当該ルータに送り込んで、ルータ上に用意されたコマンドを用いて、インターネット上の外部サイトサーバからスクリプトファイルをダウンロードさせ、実行権限を書き換えてから実行させることで当該ルータを Bot 化させる

この手口に対応した一連の攻撃パケットの増加が観測された期間が、脆弱性情報や修正パッチが公表された 2014 年 9 月以降も数回ありました。パッチの適用が進まない中で、新たに Bot 化する機器が今後も増え続け、DDoS 攻撃がさらに深刻化する恐れがあります。(*6)

3 参考文献

(1) Service Name and Transport Protocol Port Number Registry
http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml
(2) JPCERT/CC インターネット定点観測レポート(2015 年 1～3 月)
https://www.jpcert.or.jp/tsubame/report/report201501-03.html
(3) 警察庁@Police
インターネット観測結果等 (平成 27 年 5 月期)
https://www.npa.go.jp/cyberpolice/detect/pdf/20150624.pdf
(4) トレンドマイクロセキュリティブログ
UDP ポートを開放した状態にする Netis 製ルータに存在する不具合を確認
http://blog.trendmicro.co.jp/archives/9725
(5) トレンドマイクロセキュリティブログ
Netis 製ルータに存在する不具合を修正する更新プログラムを検証
http://blog.trendmicro.co.jp/archives/10050
(6) Shadow Server
Vulnerable Netis Router Scanning Project
https://netisscan.shadowserver.org/

本活動は、経済産業省より委託を受け、「平成２６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。

本文書を引用、転載する際には JPCERT/CC 広報(office@jpcert.or.jp)まで確認のご連絡をお願いします。最新情報については JPCERT/CC の Web サイトをご参照ください。

JPCERT コーディネーションセンター(JPCERT/CC)
https://www.jpcert.or.jp/tsubame/report/index.html