Japan Computer Emergency Response Team Coordination Center

電子署名 : 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 : 2016.08.24 14:44:39 +09'00'

JPCERT-IA-2016-03

発行日 ： 2016-08-25

JPCERT/CC インターネット定点観測レポート
[2016 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。

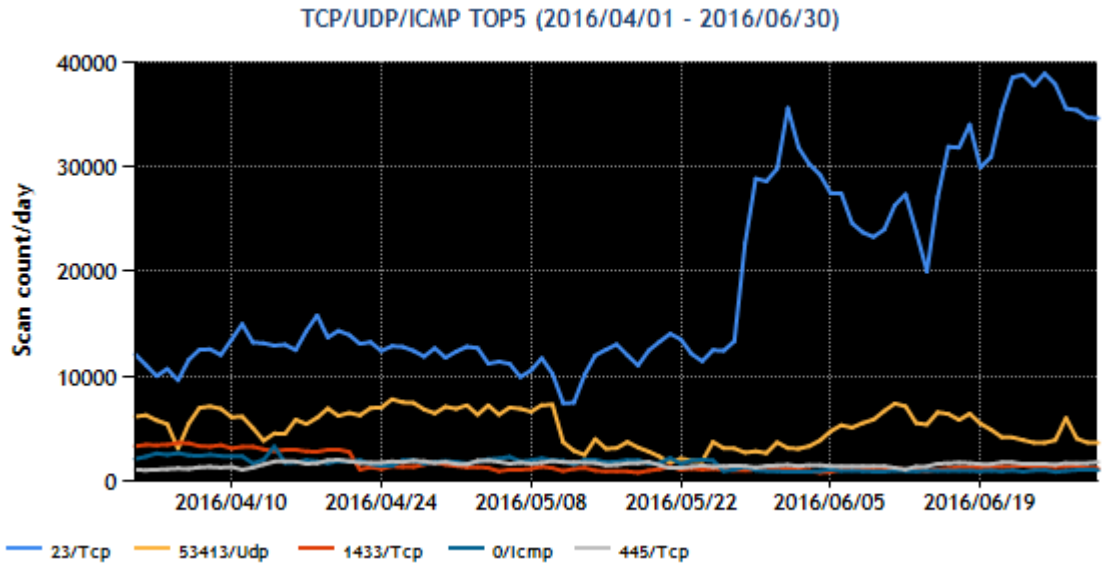
宛先ポート番号別パケット観測数のトップ 5 を ［表 1］に示します。

［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	53413/UDP	2
3	1433/TCP (ms-sql-s)	5
4	0/ICMP	3
5	445/TCP (microsoft-ds)	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。



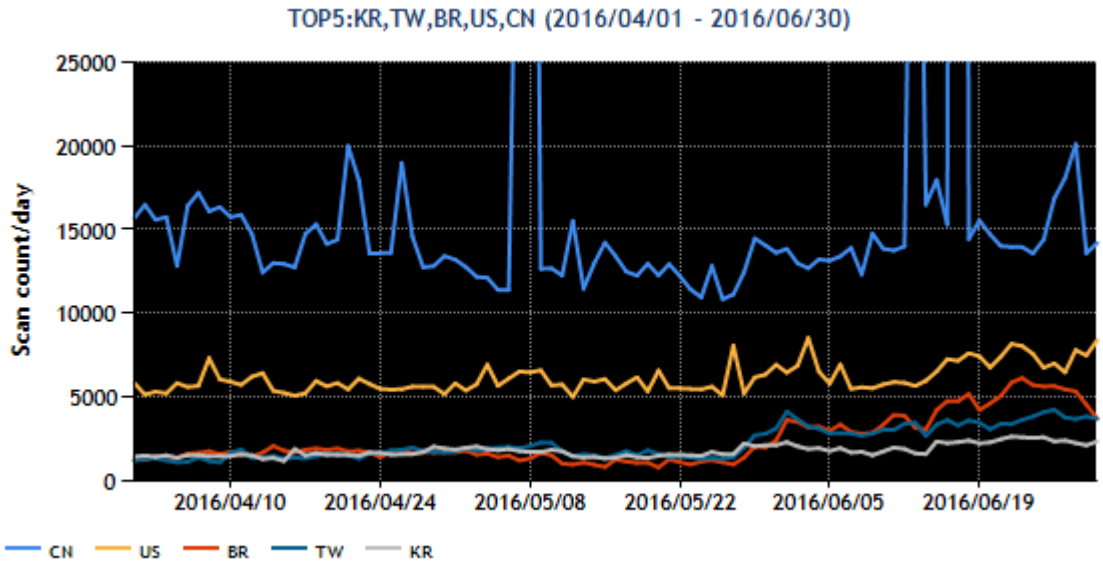
［図 1：2016 年 4～6 月の宛先ポート番号別パケット観測数トップ 5 の推移］

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	ブラジル	7
4	台湾	4
5	韓国	3

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。



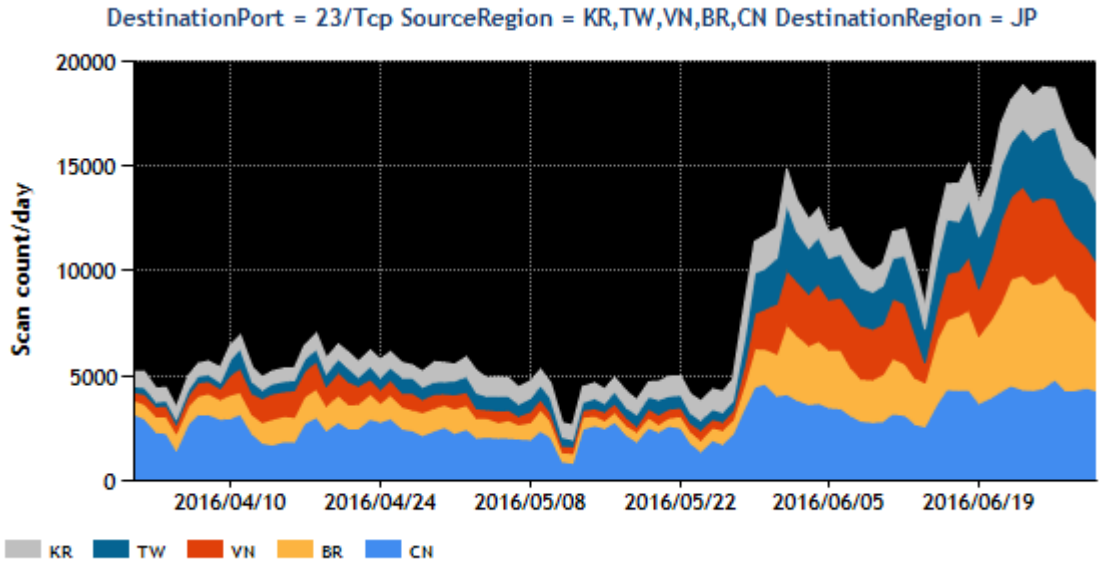
［図 2：2016 年 4～6 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

本四半期は、23/TCP 宛のパケットが 5 月 27 日ごろより急増しています。この現象については、2.1「Port23/TCP 宛のパケット数の増加」で詳しく述べます。宛先ポート番号のトップ 5 については、特筆すべき内容はありません。次に、送信元地域別のトップ 5 ですが、前四半期パケット数で 7 番目の送信元だったブラジルが、3 番目に浮上しています。これはブラジルを送信元とする 23/TCP 宛のパケットが数多く観測されているためであり、23/TCP の送信元地域としては 2 番目となっています。その他の地域については、多少の増減はありましたが、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　Port23/TCP 宛のパケット数の増加

2016 年 5 月 27 日ごろより、Port23/TCP 宛に対するパケット数の増加を観測しています。特定の地域に限らず複数の地域からのパケットが増加しています。（図 3）



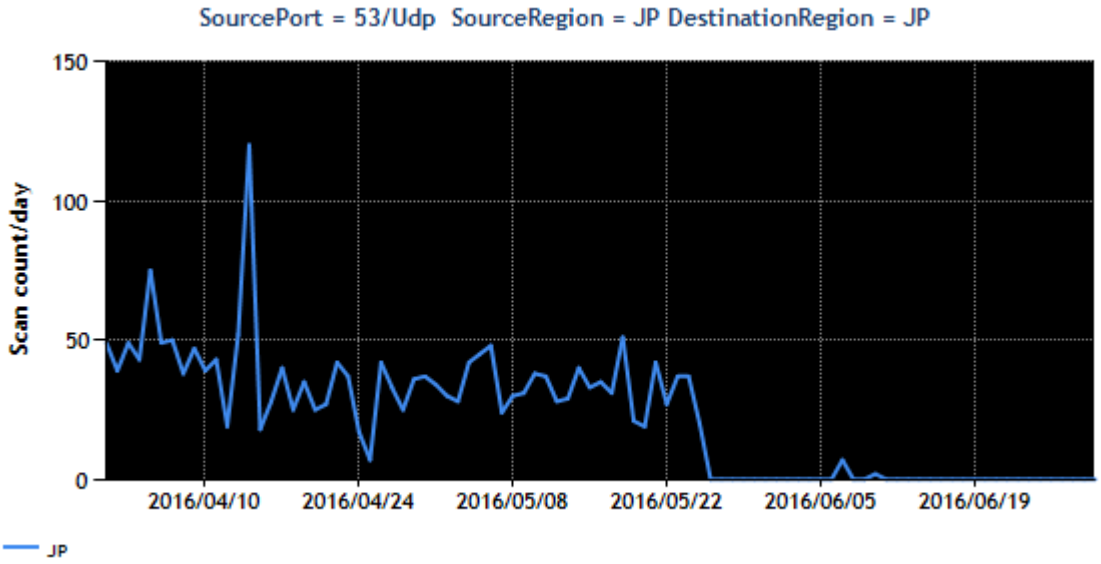
［図 3. Port23/TCP 宛のパケット数の推移］

5 月 27 日以降に増加したパケットのケースでは、送信元となっている IP アドレスに、認証用 Web インターフェースを表示する CCTV などの機器の存在を確認しました。CCTV とみられる機器については、日本国内の複数の製品からも不審なパケットが送られていることを確認しています。こうした調査結果に基づいて、製品の開発者には製品の問題を、稼働中の機器が設置されている IP アドレスの管理者には稼働中の製品の問題を解消いただくよう JPCERT/CC から連絡しました。

このように、JPCERT/CC では、不審なパケットの送信元 IP アドレスに設置されている機器を調査して機種を推定し、必要に応じて当該機器の製造ベンダ等や、関連 ISP 等に情報を提供し、問題点の解消に努めています。そうした事例を「JPCERT/CC インターネット定点観測レポート」[(*2)]でも、これまで数回にわたって紹介しております。

2.2　国内のオープンリゾルバ等を使った DNS 水責め攻撃の減少

DNS のクエリに対するリプライパケットを TSUBAME が、国内外の多数の IP アドレスから受信しています。受信したパケットを分析したところ、存在しないランダムなホスト名を含んだ名前解決要求パケットに対する応答パケットであることが分かりました。これは、DNS 水責め攻撃のために、TSUBAME のセンサーの IP アドレスを詐称して、オープンリゾルバに第三者が送信した名前解決要求パケットに対する応答パケットと考えられます(*3)。送信元ポートが Port53/UDP のパケット数の推移を図 4 に示します。



［図 4. 53/UDP からのパケット観測数の推移］

5 月 25 日以降は、日本国内のオープンリゾルバ等を使った DNS 水責め攻撃とみられるパケットが観測されなくなりました(*4)。BIND 等 DNS 用ソフトウエアや、DNS 事業者等の対策が進んだためとも、本手法を攻撃者が用いなくなったためとも考えられますが、真相は不明です。
再びオープンリゾルバを使った DNS 水責め攻撃活動が再開される可能性もあるため、JPCERT/CC では今後も Port53/UDP のパケットの観測数の推移を注視し異常が見つかれば対処する予定です。

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) インターネット定点観測レポート
https://www.jpcert.or.jp/tsubame/report/index.html

(3) Internet Infrastructure Review（IIR）Vol.31
http://www.iij.ad.jp/company/development/report/iir/031/01_03.html

(4) DNS 水責め（Water Torture）攻撃対策と動向について 2016
http://dnsops.jp/event/20160624/DNS_Summer_Days_2016_suematsu.pdf

本活動は、経済産業省より委託を受け、「平成 28 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。