JPCERT-IA-2015-01
発行日 : 2015-01-27

JPCERT/CC インターネット定点観測レポート
[2014 年 10 月 1 日～12 月 31 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。

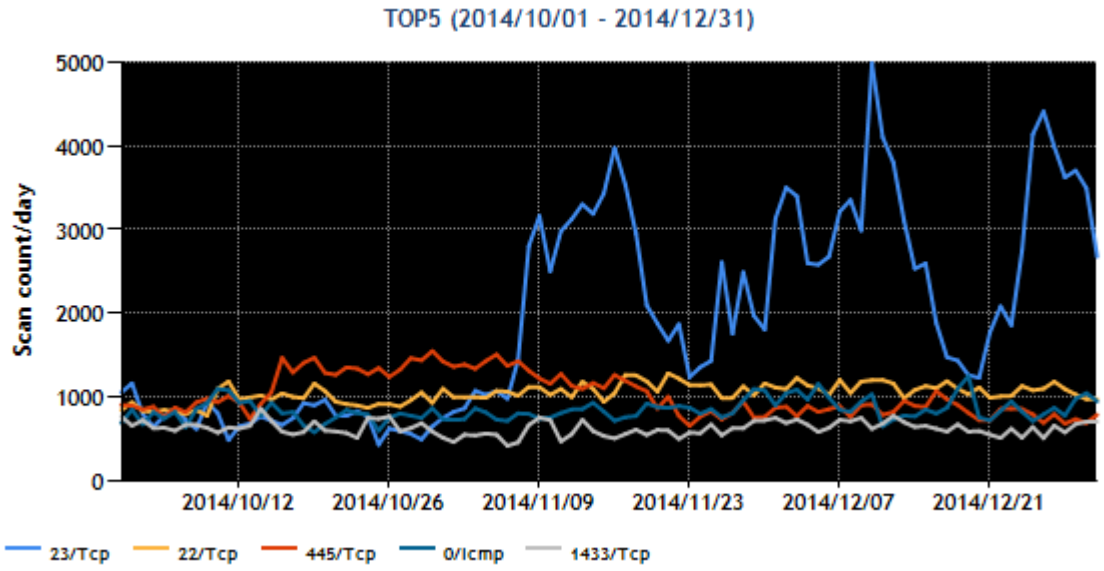
宛先ポート番号別パケット観測数のトップ 5 を [表 1]に示します。

[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	22/TCP(ssh)	3
3	445/TCP (microsoft-ds)	2
4	0/ICMP	4
5	1433/TCP (ms-sql-s)	5

※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。



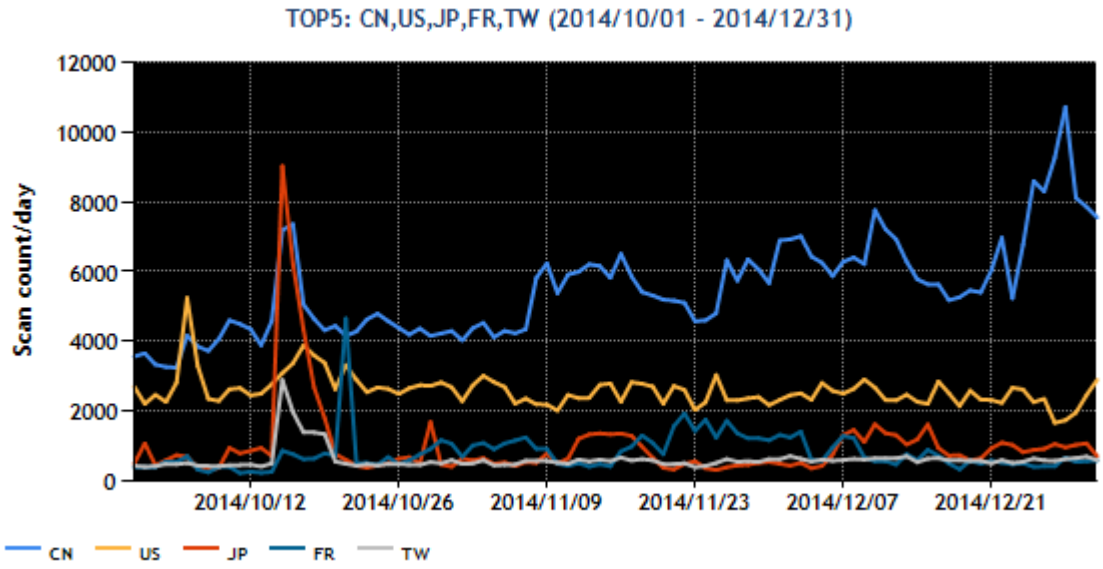
[図 1：2014 年 10~12 月の宛先ポート番号別パケット観測数トップ 5]

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	日本	5
4	フランス	9
5	台湾	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。



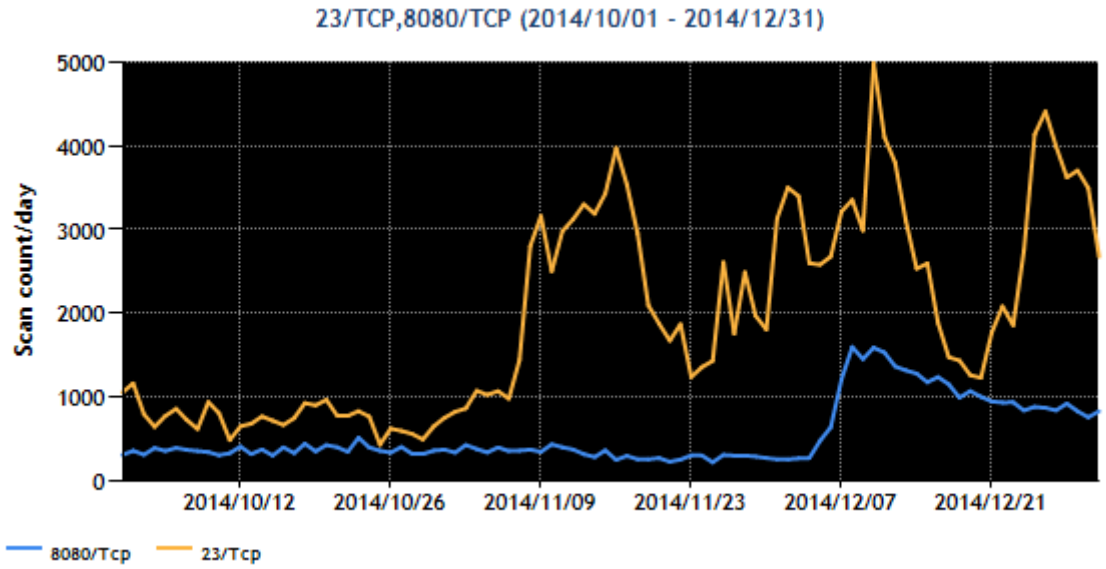
[図 2：2014 年 10~12 月の送信元地域別トップ 5 ごとのパケット観測数]

23/TCP 宛のパケット数は、11 月上旬に増加し、その状態が約一週間続いたあと減少しましたが、12 月に入ってからも数回大きな増減を繰り返しながら大量に観測される状態が続き、本四半期の合計でも最多となりました。これについては 2.1 で詳しく述べます。
10 月中旬には日本を送信元とするパケット数が増加しました。しかしながら、これは特定のセンサーが P2P ソフトウエアの通信先にされて 12543/TCP と 12543/UDP 宛の大量のパケットを一時的に受信した影響だと推測され、このセンサー以外では顕著な変化が見られなかったことから、広域的な脅威を示すデータではないと判断しています。その他については、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

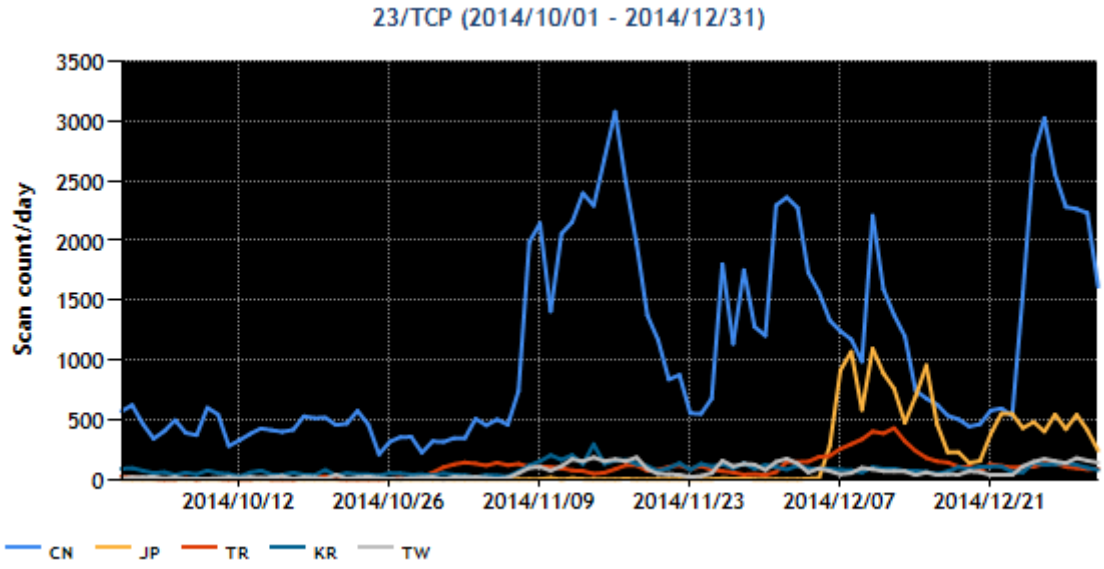
2.1　23/TCP, 8080/TCP 宛へのパケットの増加

図 3 が示すように、11 月上旬から 23/TCP 宛へのパケット数は、増減を繰り返しながら増加しています。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[*2,3,4,5] でも紹介しましたが、再び活発になっています。また、12 月上旬には 8080/TCP 宛のパケットが増加しました[*6,7,8]。



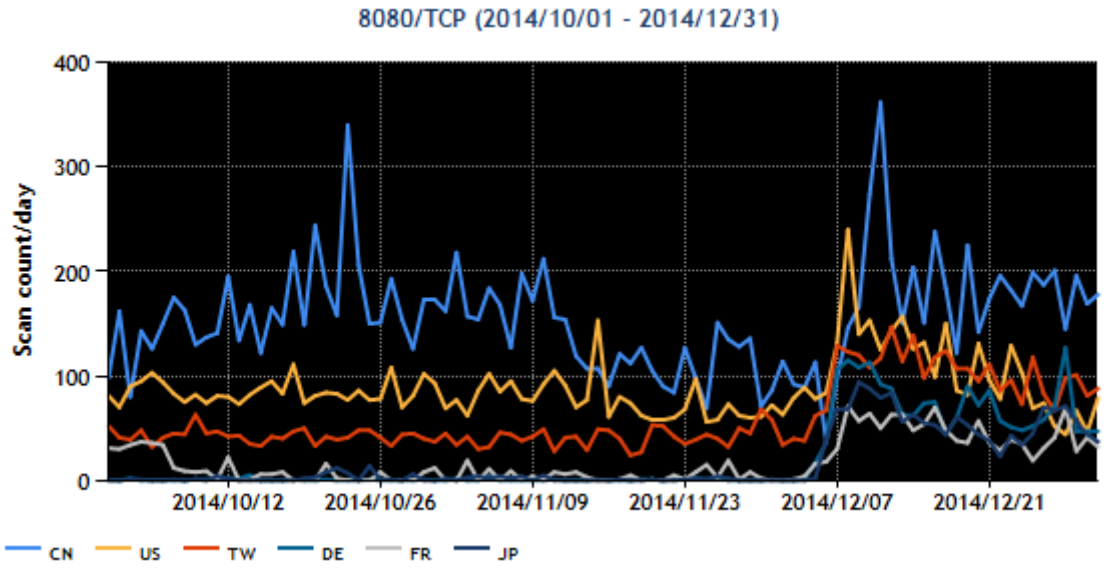
[図 3：2014 年 10～12 月の 23/TCP, 8080/TCP 宛のパケット観測数]

本四半期における 23/TCP 宛のパケットの主な送信元地域ごとの観測数の推移を図 4 に示します。送信元地域が中国であるパケットが多数を占めていますが、12 月上旬には送信元地域が日本であるパケットが増加しました。



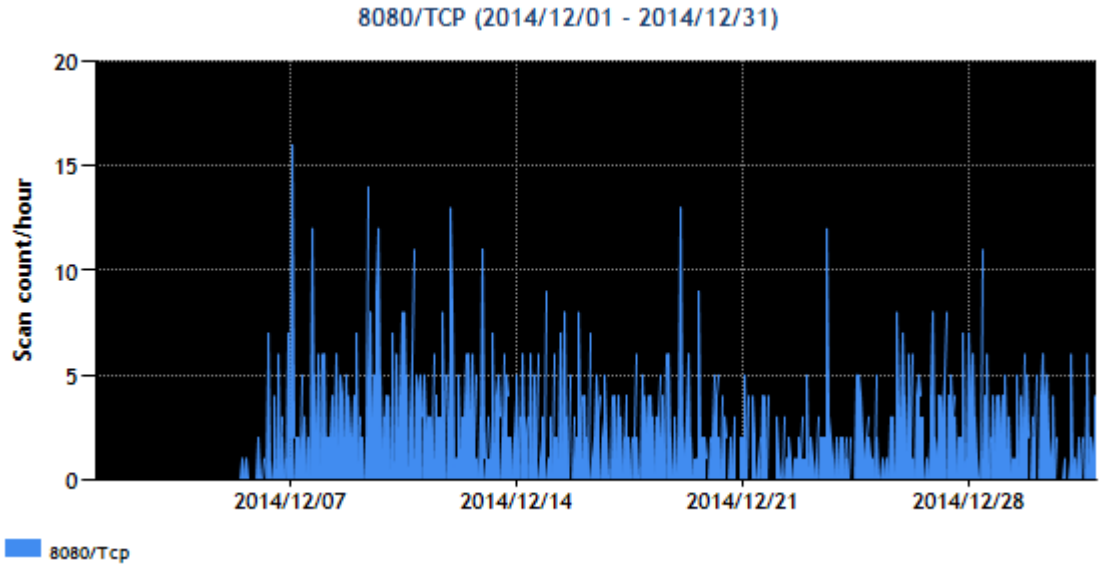
[図 4：2014 年 10～12 月の 23/TCP 宛のパケット観測数(送信元地域別)]

本四半期における 8080/TCP 宛のパケットの主な送信元地域ごとの観測数の推移を図 5 に示します。中国が最も多く、11 月上旬から増減を繰り返しています。その他のアメリカ(2 位)、台湾(3 位)、ドイツ(4 位)、フランス(5 位)は、12 月上旬を境に増加し、日本(6 位)も同じような傾向を示しています。



[図 5：2014 年 10～12 月の 8080/TCP 宛のパケット観測数(送信元地域別)]

図 6 は、送信元が日本の 8080/TCP 宛のパケットの観測数の推移を示しています。



[図 6：2014 年 12 月の 8080/TCP 宛のパケット観測数(送信元地域日本)]

これらのパケットの一部について送信元ノードを調査し、確認できたところでは、11 月までは、2014 年 1～3 月期の本レポートで (*2) で紹介した、ネットワークカメラ製品および国外で使用されている特定のブロードバンドルータ製品がほとんどでしたが、11 月下旬からは、それらに加えて QNAP 社の NAS 製品 (以下、「QNAP NAS」といいます。) が多く見られるようになりました。23/TCP および 8080/TCP 宛のパケットの送信元 IP アドレスから、日本、韓国、台湾、アメリカ、ドイツ、フランスの各地域に設置された QNAP NAS が確認できました。

8080/TCP ポートは、QNAP NAS の管理画面の標準ポートとして利用されています。また、QNAP NAS では、shell として GNU bash が使われており、古いバージョンのファームウェアを使用している場合、9 月下旬に公表 (*9) された脆弱性の影響を受けます。この脆弱性を悪用すれば QNAP NAS で任意のコードを実行できます(*10,11,12)。11 月下旬以降の 8080/TCP 宛のパケットを調査したところ、QNAP NAS の GNU bash の脆弱性に対する攻撃と推測されるリクエストであることが確認できました。

11 月下旬から観測している 23/TCP、8080/TCP 宛のパケットは、GNU bash の脆弱性を悪用して乗っ取られた QNAP NAS が、同脆弱性をもつ他の QNAP NAS などを探索するための踏み台にされて、送信していたものと推測されます。また、数は少ないものの 12 月下旬より、これらの QNAP NAS が 10000/TCP 宛のパケットを送信していることも確認しています。このパケットは脆弱な QNAP NAS のみを対象としており、QNAP NAS 以外の製品では、例え GNU bash の脆弱性をもっていても、影響を受けないと思われます。

QNAP NAS においてリモートアクセスできるようにする myQNAPcloud サービスが有効になっている場合（インストール方法によっては、標準のセットアップ手順で、myQNAPcloud サービスの設定が行われ、意図せず有効になっている可能性があります）には、「TCP 8080 番ポートへのスキャンの増加に関する注意喚起」(*13)を参考に適切なセキュリティ対策 (ファームウェアバージョンの確認やアップデート、攻撃の影響の確認など) を実施して、攻撃の踏み台に使用されないよう努めてください。

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(2012 年 1～3 月)
https://www.jpcert.or.jp/tsubame/report/report201201-03.html
(3) JPCERT/CC インターネット定点観測レポート(2012 年 4～6 月)
https://www.jpcert.or.jp/tsubame/report/report201204-06.html
(4) JPCERT/CC インターネット定点観測レポート(2014 年 1～3 月)
https://www.jpcert.or.jp/tsubame/report/report201401-03.html
(5) JPCERT/CC インターネット定点観測レポート(2014 年 7～9 月)
https://www.jpcert.or.jp/tsubame/report/report201407-09.html
(6) @police Bash の脆弱性を標的としたアクセスの観測について（第 3 報）
http://www.npa.go.jp/cyberpolice/topics/?seq=15063
(7) @police インターネット観測結果等(平成 26 年 11 月期)
http://www.npa.go.jp/cyberpolice/detect/pdf/20141218.pdf
(8) @police インターネット観測結果等(平成 26 年 12 月期)
http://www.npa.go.jp/cyberpolice/detect/pdf/20150113.pdf
(9) GNU bash の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2014/at140037.html
(10) Protect Your Turbo NAS from Remote Attackers - Bash (Shellshock) Vulnerabilities
http://www.qnap.com/i/en/support/con_show.php?cid=61
(11) An Urgent Fix on the Reported Infection of a Variant of GNU Bash Environment Variable Command Injection Vulnerability
http://www.qnap.com/i/jp/support/con_show.php?cid=74
(12) The Shellshock Aftershock for NAS Administrators
https://www.fireeye.com/blog/threat-research/2014/10/the-shellshock-aftershock-for-nas-administrators.html
(13) TCP 8080 番ポートへのスキャンの増加に関する注意喚起
https://www.jpcert.or.jp/at/2014/at140055.html

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。