JPCERT-IA-2014-02
発行日 : 2014-07-17

JPCERT/CC インターネット定点観測レポート
[2014 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。

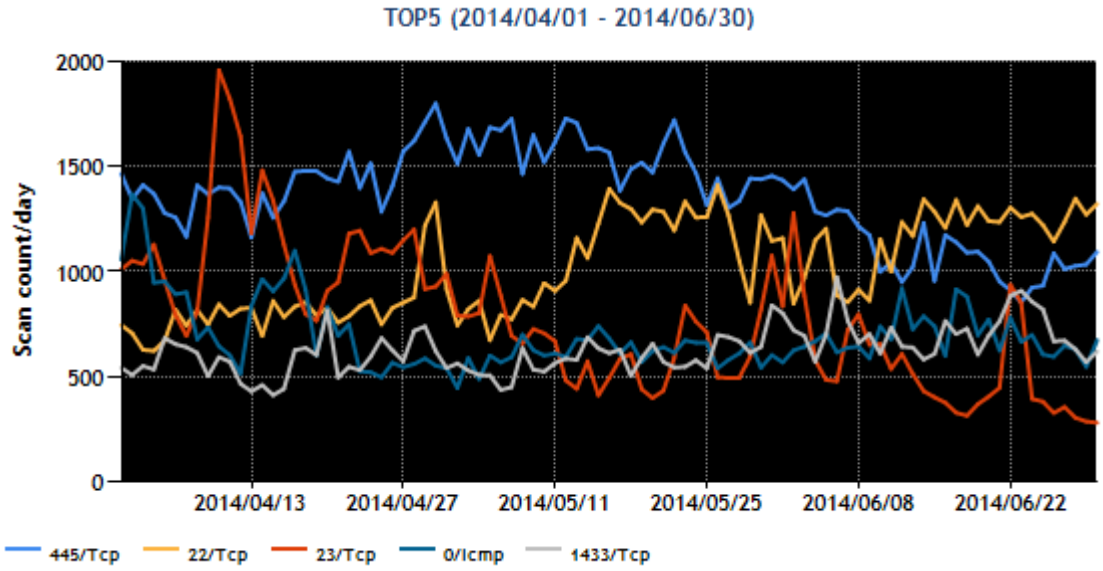
宛先ポート番号別パケット観測数のトップ 5 を [表 1]に示します。

[表 1 : 宛先ポート番号トップ 5]

宛先ポート番号	本四半期順位	前四半期順位
445/TCP (microsoft-ds)	1	1
22/TCP (ssh)	2	3
23/TCP (telnet)	3	2
0/ICMP	4	4
1433/TCP (ms-sql-s)	5	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時間的な変化を示しています。



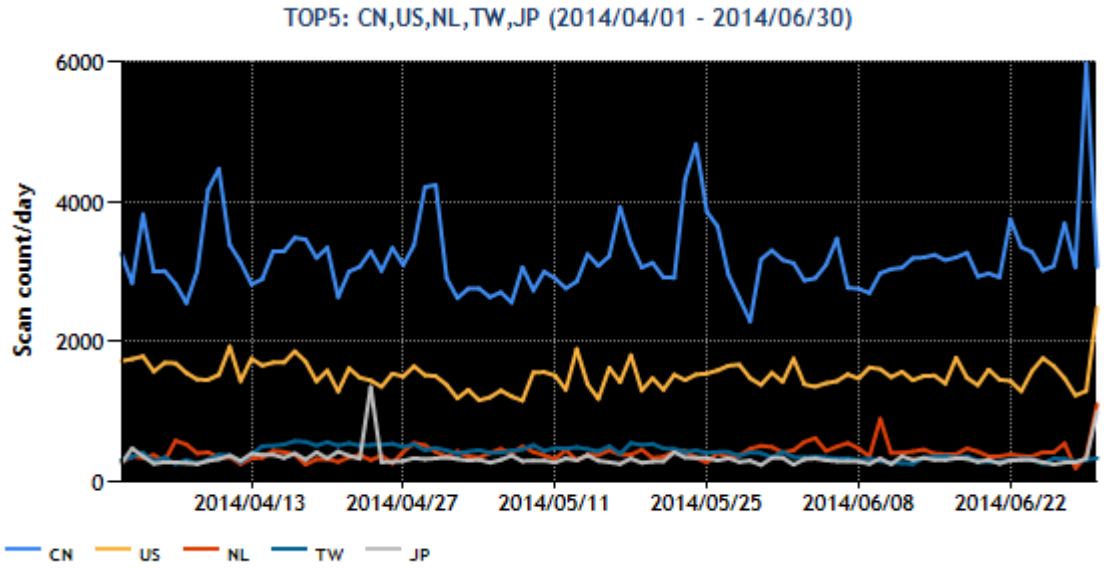
[図 1：2014 年 4~6 月の宛先ポート番号別パケット観測数トップ 5]

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]

送信元地域	本四半期順位	前四半期順位
中国	1	1
米国	2	2
オランダ	3	4
台湾	4	6
日本	5	3

図 2 に期間中のパケット送信元地域トップ 5 の変化を示します。



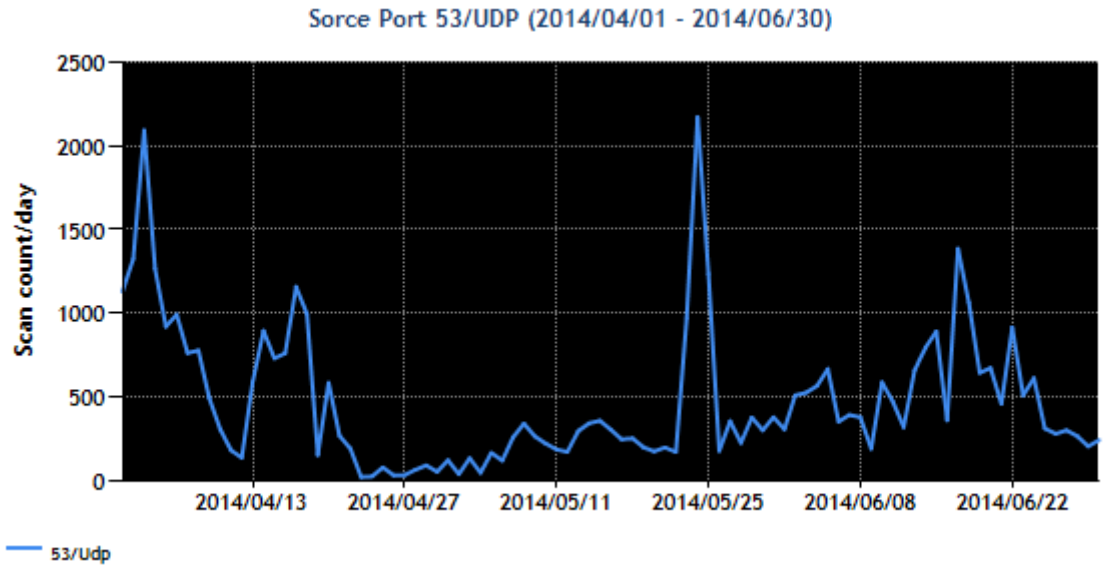
[図 2：2014 年 4~6 月の送信元地域別トップ 5]

本四半期は、22/TCP 宛のパケット数が徐々に増加しました。23/TCP については、前四半期の(2 番目)から減少して 3 番目にはなりましたが、依然として多いと言える状態です。その他については、多少の増減はありますが、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　DNS の応答パケットおよび DNS サービスのポートの不達を示す ICMP エラーパケットの観測

送信元ポート番号が 53/UDP を使用するパケット(以下「DNS 応答パケット」といいます。)と、DNS サービスのポート不達を示す ICMP エラーパケット(Destination unreachable)を本四半期も多数観測しました。



[図 3：2014 年 4~6 月の送信元ポート番号 53/UDP のパケット観測数]

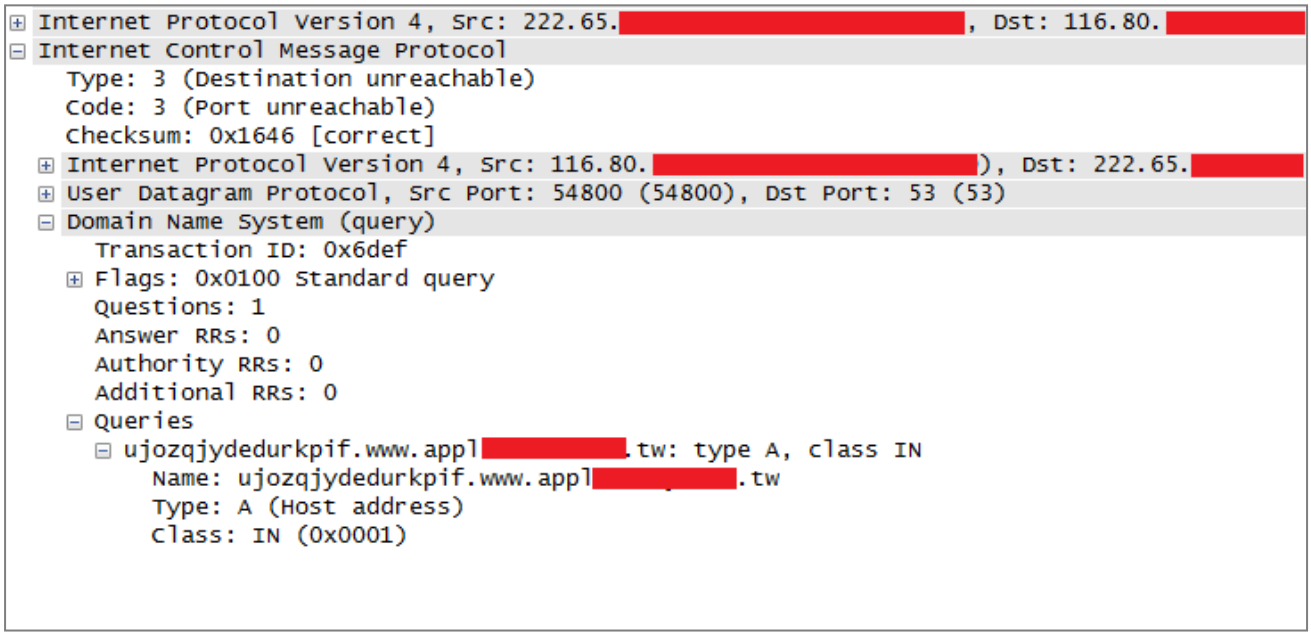
センサーが受信した DNS 応答パケットを分析したところ、図 4 のような(不規則な文字の羅列が含まれる)実際には存在しない FQDN の問い合わせに対する応答でした。

```
⊞ Internet Protocol Version 4, Src: 24.181.[redacted], Dst: 116.80.[redacted]
⊞ User Datagram Protocol, Src Port: 53 (53), Dst Port: 54800 (54800)
⊟ Domain Name System (response)
    Transaction ID: 0x6def
  ⊞ Flags: 0x8183 Standard query response, No such name
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ mlafmfohepqh.www.appl[redacted].tw: type A, class IN
        Name: mlafmfohepqh.www.appl[redacted].tw
        Type: A (Host address)
        Class: IN (0x0001)
```

[図 4：2014 年 6 月の送信元ポート番号 53/UDP のパケット(Wireshark による表示)]

これらの DNS 応答パケットは、不特定のホスト(インターネット経由)からの再帰的な問い合わせを許可しているキャッシュ DNS サーバや、不特定のホストからの DNS 問い合わせに対しても ISP などのキャッシュ DNS サーバに転送(DNS フォワーダ機能)してしまう機器(以下、両者を「オープンリゾルバ」といいます。)経由で、存在しない多数の FQDN を問い合わせて攻撃対象の権威 DNS サーバに過剰な負荷

を加えようと攻撃者が送った DNS 問い合わせパケットに対する応答であり、攻撃者によって詐称された送信元 IP アドレスが、偶然センサーに割り当てられた IP アドレスだったために、センサーに受信されたと推測されます。すなわち、権威 DNS サーバを狙った DDoS 攻撃の余波を観測しています。

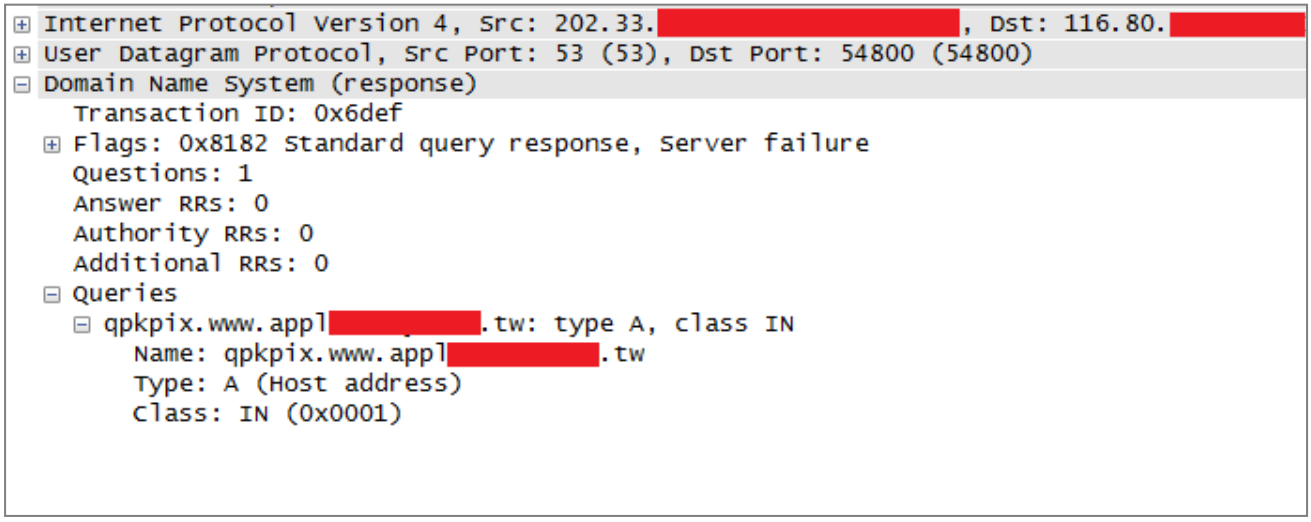


[図 5：2014 年 6 月の送信元ポート番号 53/UDP に対する ICMP エラー(Wireshark による表示)]

一方、DNS サービスのポート番号宛の不達を示す ICMP エラーパケット(図 5)は、上述の攻撃に使おうとしたノードの一部が、既にオープンリゾルバでなくなっていたなどのために、攻撃パケットが通過できず、その不達を示す ICMP エラーパケットが、センサーに届いたものと見られます。

DDoS 攻撃の標的と見られる権威 DNS サーバは、国外の複数のドメインで、ニュースサイトやインターネット投票サイト、 CDN (Contents Delivery Network) など様々でした。現時点では、国内のドメインが攻撃対象となった事例は確認できていません。しかしながら、この攻撃には、多数の国内のオープンリゾルバが悪用されており、意図的ではないにせよ攻撃に加担する結果となっていることが由々しき問題です。

さらに、攻撃に加担したオープンリゾルバは、攻撃対象となっている権威 DNS サーバだけではなく、オープンリゾルバと権威 DNS サーバ間にある ISP 等が提供しているキャッシュ DNS サーバの負荷も押し上げます。これにより、同じキャッシュ DNS サーバを利用しているクライアントからの問い合わせに対して図 6 のようなエラー(Server failure)などを返して、Web サイトの閲覧やメールの送信などができなくなる可能性もあります。



[図 6：2014 年 6 月の送信元ポート番号 53/UDP のパケット(Wireshark による表示)]

上で述べたような攻撃の踏み台となっているオープンリゾルバを減らすために、特に次の点について注意してください。

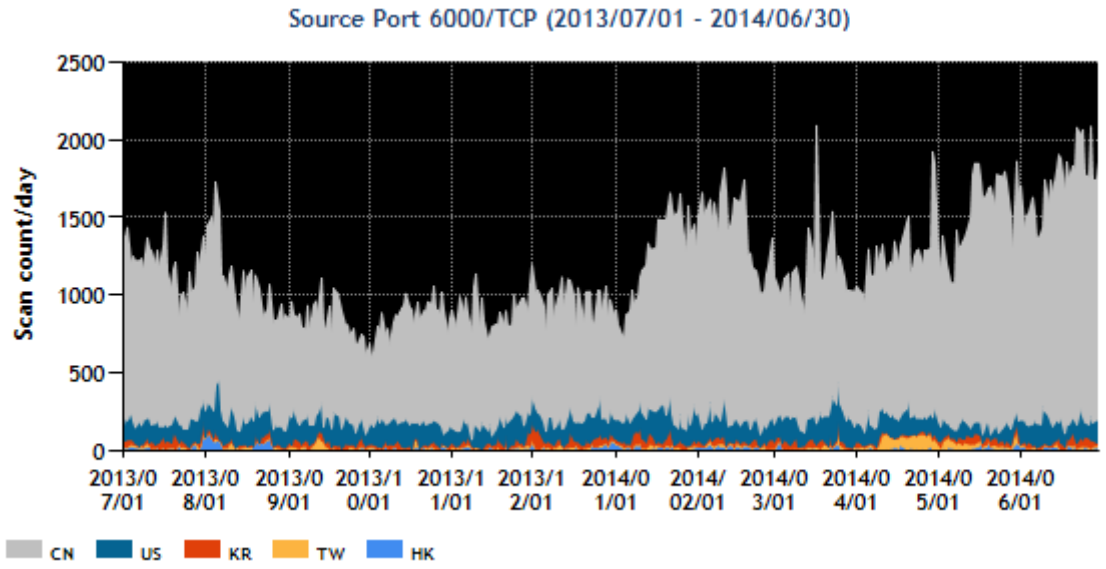
1. DNS サーバを運用している場合は、再帰的な問い合わせを受け付ける範囲など、設定を再確認し、必要最小限になるようアクセス制限を施してください。(*2, 3, 4)

2. インターネット接続用ルータなどで DNS サーバや DNS フォワーダ機能を持つネットワーク機器を使用している場合は、不特定のホストからの DNS 問い合わせに応答しない設定になっていることを確認してください。各製品ベンダから公開されている情報を参考に、設定の確認をお勧めします。(*4, 5)

3. Web サーバなどの公開サーバを運用している場合は、管理するサーバで不要な DNS サーバが稼働していないか念のため確認してください。

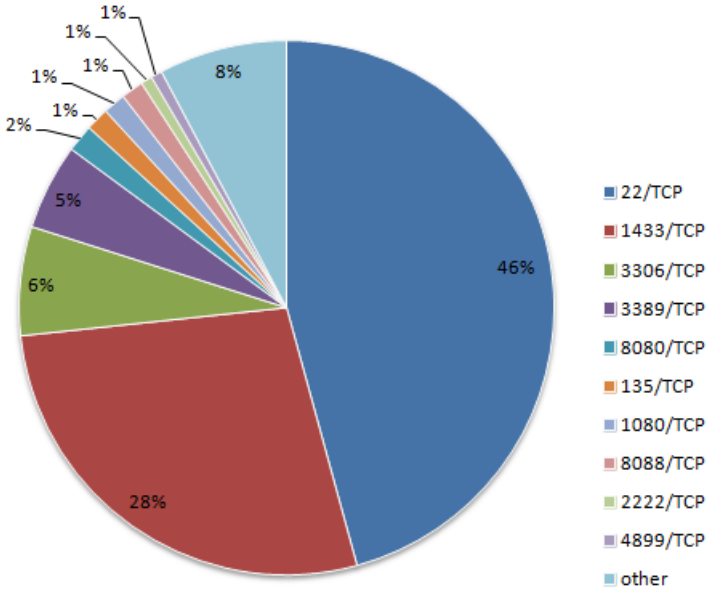
2.2 送信元ポート番号 6000/TCP のパケット

2013 年第四四半期(2014 年 1 月)頃から送信元ポート番号が 6000/TCP とするパケット数が右肩上がりに増加しています。本四半期における日本宛の全パケット数のうち約 2 割を占め、他を上回っています。また、これらのパケットの送信元地域は中国が多くを占めています。



[図 7：2013 年 7 月~2014 年 6 月の送信元ポート番号 6000/TCP のパケット観測数]

送信元ポート番号を 6000/TCP とするこれらのパケットは、攻撃活動や準備活動などを目的としたものが多数を占めています。図 8 は、本四半期の送信元ポート番号を 6000/TCP としたパケットの宛先ポート番号の内訳です。



[図 8：2014 年 4~6 月の送信元ポート番号 6000/TCP とした宛先ポート番号の割合]

[表 3：送信元ポート番号 6000/TCP としたパケットの宛先ポート番号のトップ 10]

本四半期順位	宛先ポート番号
1	22/TCP (ssh)
2	1433/TCP (ms-sql-s)
3	3306/TCP(mysql)
4	3389/TCP(ms-wbt-server)
5	8080/TCP (http-alt)
6	135/TCP (epmap)
7	1080/TCP (socks)
8	8088/TCP (radan-http)
9	2222/TCP (EtherNet-IP-1)
10	4899/TCP (radmin-port)

※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。

これらの送信元ポート番号 6000/TCP とするパケットを分析したところ、1 つの送信元 IP アドレスから、特定の送信先の IP アドレスに対し規則的(数日に 1 回 1 パケットずつ)に送信されていること、Window サイズが特定の値で固定されていることなどから海外製の特定ツールによる探索活動である可能性が高いことが分かりました。(*6, 7)

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) 株式会社日本レジストリサービス(JPRS)
DNS サーバーの不適切な設定「オープンリゾルバー」について
http://jprs.jp/important/2013/130418.html
(3) 日本ネットワークインフォメーションセンター
オープンリゾルバ(Open Resolver)に対する注意喚起
https://www.nic.ad.jp/ja/dns/openresolver/
(4) JPCERT/CC
オープンリゾルバ確認サイト
http://www.openresolver.jp/
(5) JVN#62507275 複数のブロードバンドルータがオープンリゾルバとして機能してしまう問題
https://jvn.jp/jp/JVN62507275/
(6) 警察庁@Police
情報技術解析平成 25 年報 別冊資料 インターネット観測結果等について
http://www.npa.go.jp/cyberpolice/detect/pdf/H25_betsu.pdf
(7) 警察庁@Police
インターネット観測結果等 (平成 25 年 11 月期)
http://www.npa.go.jp/cyberpolice/detect/pdf/20140206_2.pdf

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。