JPCERT CC®

2013 年 10 月 24 日

JPCERT/CC インターネット定点観測レポート
[2013 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います。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、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。

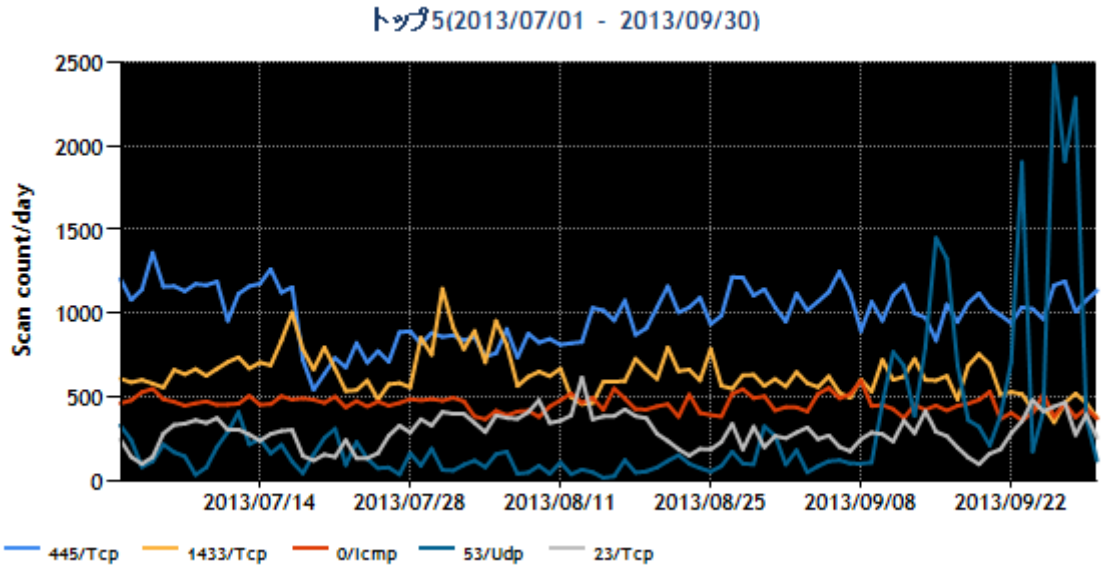
本四半期（2013 年 7 月 1 日から 9 月 30 日）に観測した宛先ポート番号別パケット観測数のトップ 5 を[表 1]に示します。

[表 1：宛先ポート番号トップ 5]

2013 年 4～6 月		2013 年 7～9 月	
1	445/TCP	1	445/TCP
2	1433/TCP	2	1433/TCP
3	0/ICMP	3	0/ICMP
4	3389/TCP	4	53/UDP
5	22/TCP	5	23/TCP

※各ポートで使用するサービス等は、3.参考文書の(*1)を参照してください。

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。



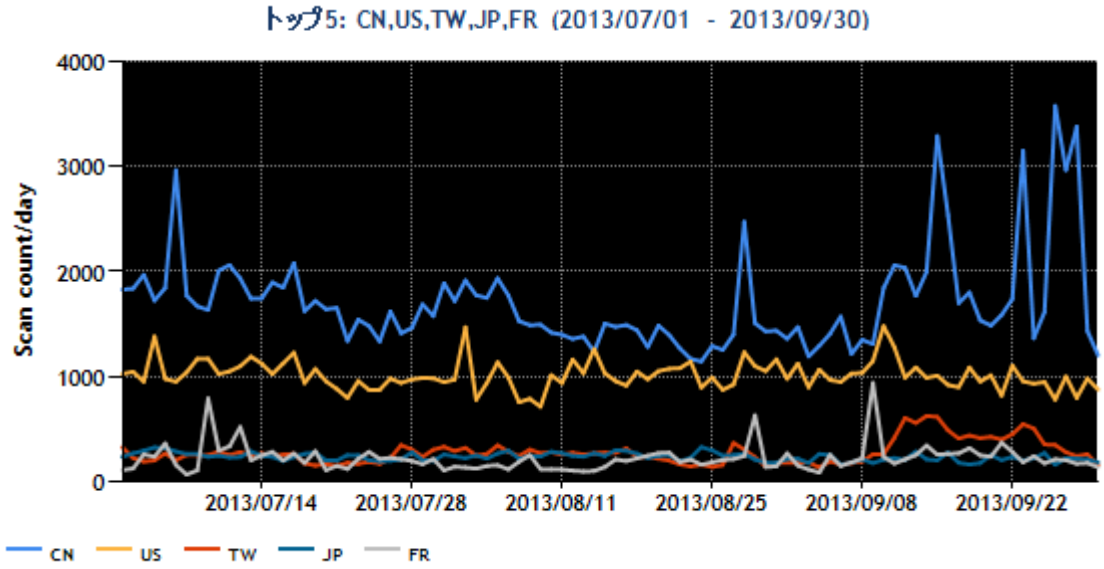
[図 1　2013 年 7~9 月の宛先ポート番号別パケット観測数トップ 5]

本四半期に観測した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]

2013 年 4～6 月		2013 年 7～9 月	
1	中国	1	中国
2	米国	2	米国
3	日本	3	台湾
4	台湾	4	日本
5	フランス	5	フランス

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　2013 年 7~9 月の送信元地域別トップ 5]

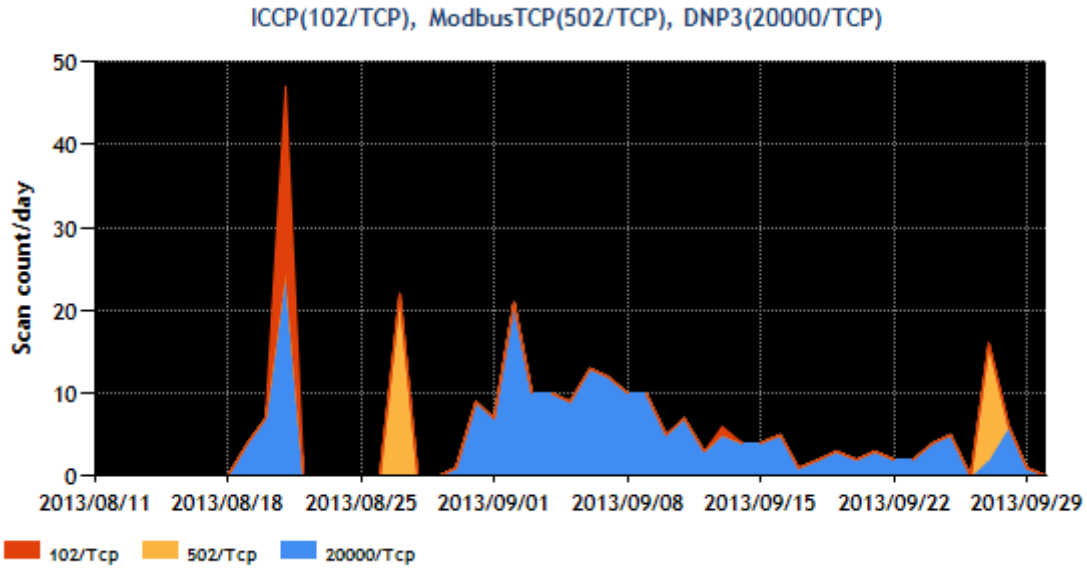
本四半期の傾向として、9 月上旬以降の中国を送信元とする 53/UDP 宛のパケットの増加が目立ちました。本現象については、「2.2」で詳しく述べます。53/UDP 以外は、多少の増減はありますが、特筆すべき状況は見られませんでした。

2　注目された現象

2.1　制御システムプロトコルに関するスキャンを観測

制御システムで使用する 102/TCP、502/TCP、20000/TCP のポート宛へのパケットを 8 月中旬以降観測しています。（制御系システムで使われるポートについては、3.参考文書の(*2)を参照してください）同時期に、SANS が提供しているグラフ (*3)(*4) (*5) でも同様の傾向がみられます。今回観測されたパケットには、①検索エンジン SHODAN (*6)の特徴的な探索パケット、②それ以外のパケットが含まれていました。

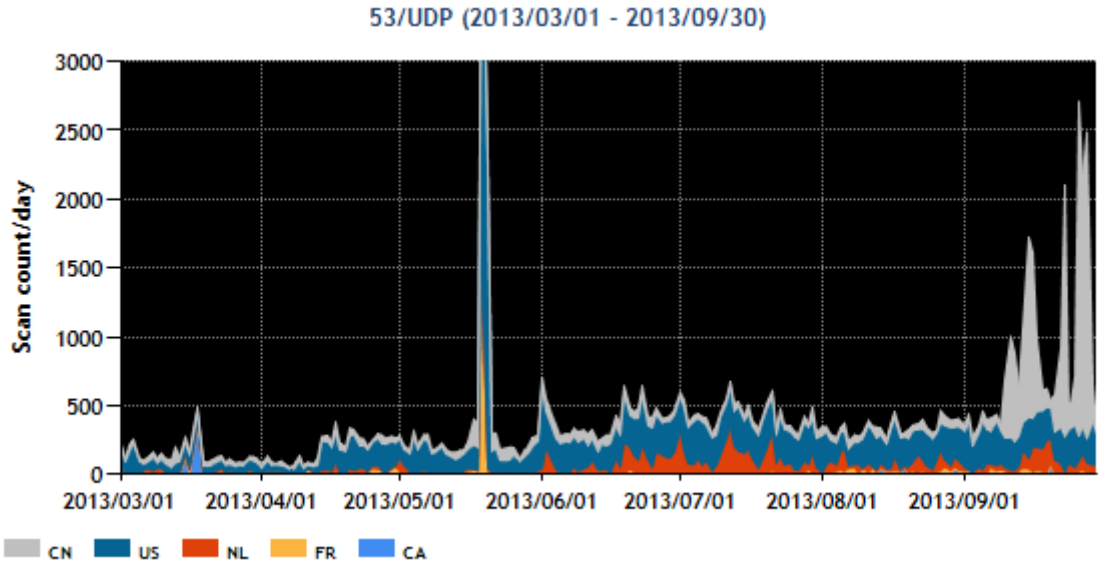
制御システムに対する攻撃者の関心を裏付けるデータであると言えます。制御システムの運用者は、直接インターネットに接続されていないか、また、ルータやファイヤーウォールなどを使用して、適切なアクセス制御がされているかを確認されるようお勧めします。



[図 3　2013 年 8～9 月の 102/Tcp,502/TCP,20000/TCP 宛のパケット観測数]

2.2　53/UDP 宛へのパケットの増加

9 月上旬以降 53/UDP 宛のパケット数が増減を繰り返しつつ過去見られなかった数を観測しています。この 53/UDP の現象は、中国の通信事業者に割り当てられた特定の 2 つの IP アドレスを送信元とした多数のパケットが原因です。これらのパケットは多数のセンサーで受信しており、同様の DNS の再帰的な問い合せでした。JPCERT/CC では、それらの問い合せを確認したところ、いずれのレコードも大きな応答を返すものでした。



[図 4　2013 年 3～9 月の 53/UDP 宛のパケット観測数]

該当パケットを分析したところ、送信元の IP アドレスが詐称されている可能性があります。複数のセンサーが受信している状況や各センサーでの受信頻度などから、今回の現象は、オープンリゾルバの状態の DNS サーバを探索する目的ではなく、インターネット上に多数存在するオープンリゾルバを使用した中国の通信事業者に割り当てられた IP アドレスを標的とした DNS Amp 攻撃が行われていたと考えられます。

このような攻撃に使用されないために、自身が運用しているサーバやネットワーク機器 (*7) で DNS キャッシュサーバが意図せず稼働していないか確認し、必要に応じて適切な対策（アップデート、パッチ、設定の変更など）を実施されることをお勧めします。

3 参考文書：

Service Name and Transport Protocol Port Number Registry (*1)
http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

Control System Port List (*2)
http://www.digitalbond.com/tools/the-rack/control-system-port-list/

SANS Internet Storm Center DShield Port Details :ICCP (*3)
https://isc.sans.edu/port.html?port=102

SANS Internet Storm Center DShield Port Details : ModbusTCP (*4)
https://isc.sans.edu/port.html?port=502

SANS Internet Storm Center DShield Port Details : DNP3 (*5)
https://isc.sans.edu/port.html?port=20000

* SANS が提供するグラフは、ブラウザで表示した時の日付を基準として 1 ヶ月前の状況を表示します。そのため、増加の状況をご覧いただく際には、Graph Criteria の Start Date を 2013-08-10 前後に設定し UPDATE をクリックし、ご確認ください。

SHODAN (*6)
http://www.shodanhq.com/

JVN#62507275 (*7)
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/index.html