Japan Computer Emergency
Response Team Coordination
Center

2014 年 3 月 31 日

JPCERT/CC インターネット定点観測レポート
[2013 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。

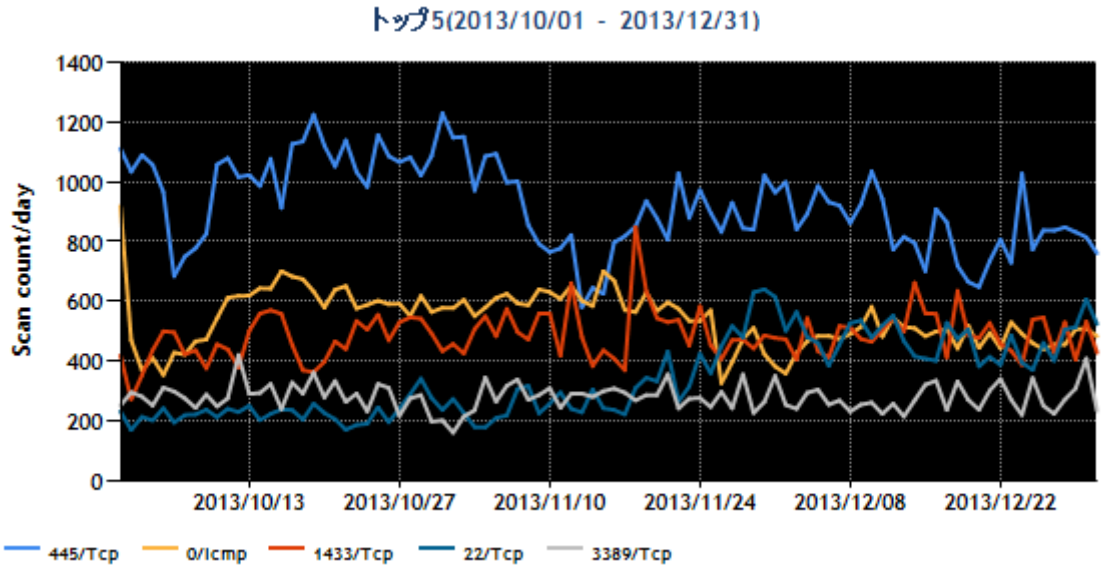
本四半期（2013 年 10 月 1 日から 12 月 31 日）に観測した宛先ポート番号別パケット観測数のトップ 5 を[表 1]に示します。

[表 1：宛先ポート番号トップ 5]

2013 年 7～9 月		2013 年 10～12 月	
1	445/TCP	1	445/TCP
2	1433/TCP	2	0/ICMP
3	0/ICMP	3	1433/TCP
4	53/UDP	4	22/TCP
5	23/TCP	5	3389/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。



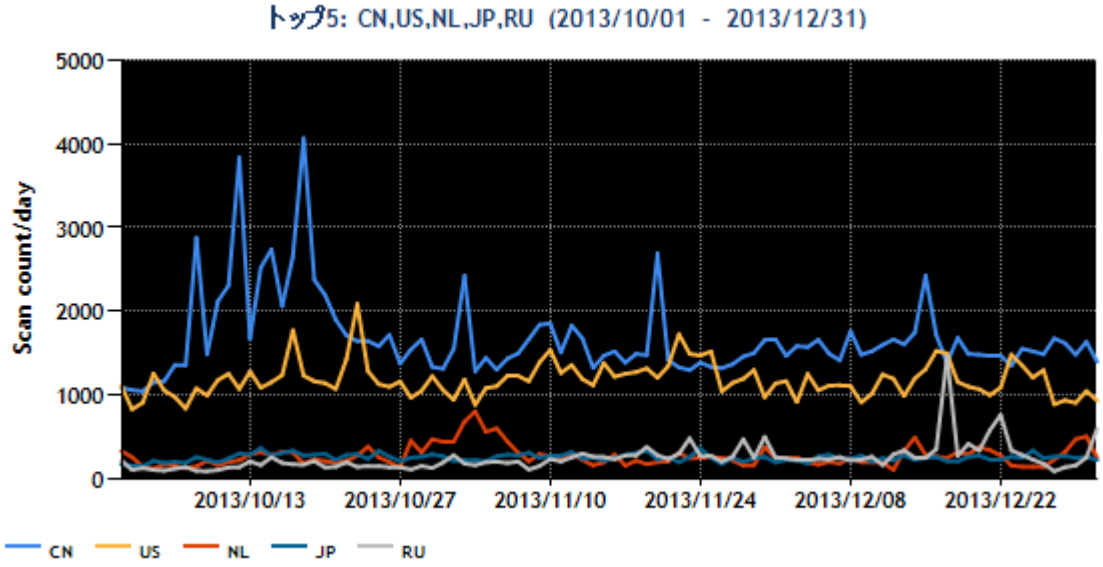
[図 1　2013 年 10~12 月の宛先ポート番号別パケット観測数トップ 5]

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 7～9 月		2013 年 10～12 月	
1	中国	1	中国
2	米国	2	米国
3	台湾	3	オランダ
4	日本	4	日本
5	フランス	5	ロシア

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。



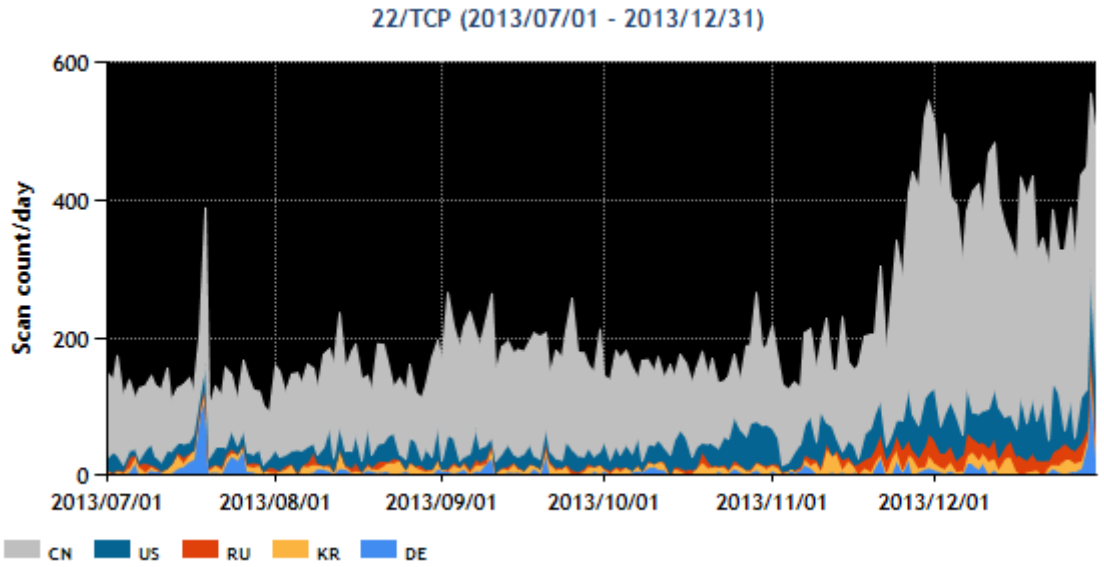
[図 2　2013 年 10~12 月の送信元地域別トップ 5]

11 月中旬以降において 22/TCP 宛のパケットが徐々に増加しました。本現象については、「2.1」で詳しく述べます。また、前四半期 4 位だった 53/UDP 宛のパケットが 10 月以降減少して本四半期では 7 位となっています。本現象については、「2.3」で詳しく述べます。その他、TOP5 には現れていませんが、80/TCP, 135/TCP 宛のパケット数が前四半期と比較して、それぞれ倍近くまで増加しています。これらの増加については推測される原因が見当たりません。

2　注目された現象

2.1　22/TCP ポート宛へのパケットの増加

11 月中旬以降、22/TCP (SSH 用)宛のパケット数が増加しています。図 3 からわかるように、中国に割り当てられた IP アドレスを送信元とするパケットが特に増えています。本四半期に受信した 22/TCP 宛のパケットのうち、送信元ポート番号が 6000/TCP のパケットが約 2 割を占めました。また、前四半期と比較してもパケット数が約 6 割増加しています。これは特定のツールによって送信されたパケットであると推測しています。

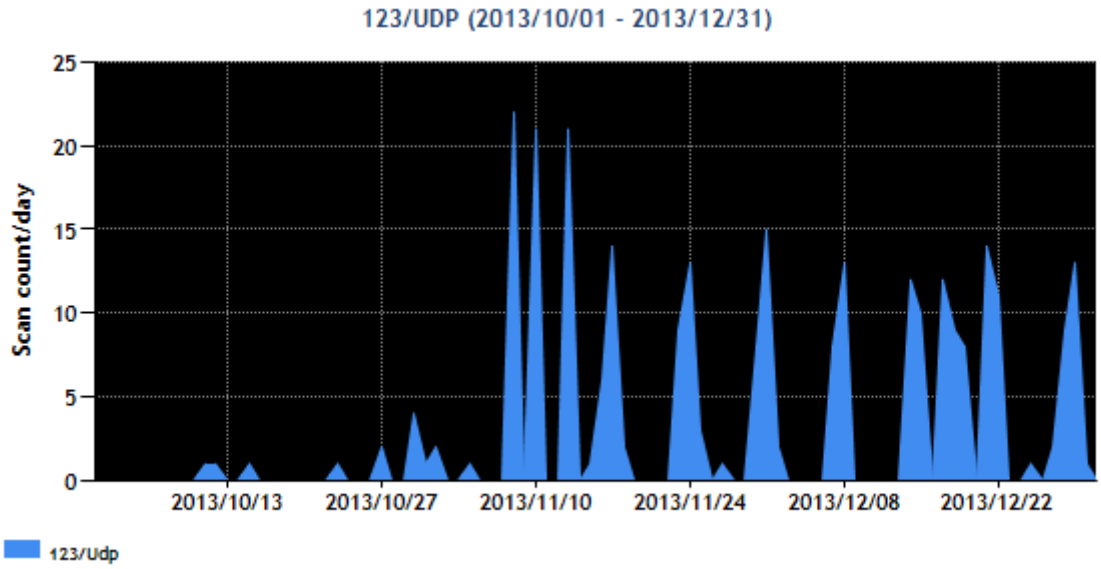


[図 3 2013 年 7～12 月の 22/TCP 宛のパケット観測数]

SSH サーバの探索や不正利用を試みる活動の活発化と見られますので、サーバ管理やインターネット経由の遠隔ログインなどで SSH を利用している場合には、パスワード認証ではなく公開鍵認証を利用するなどの対策をお勧めします。また、アクセス元が特定できる場合には、アクセス元 IP アドレスによるアクセス制限を実施してください。

2.2 123/UDP 宛へのパケットの増加

時刻同期のために使用される 123/UDP のポート宛のパケットが 11 月上旬以降増加しています。図 4 に示したように、パケット数は多くはありませんが、受信したパケットの一部には、NTP サーバの状態を問い合わせる monlist のリクエストが含まれていました(*2)。これは、DDoS 攻撃に使用できる NTP サーバを探索するための活動と推測されます。



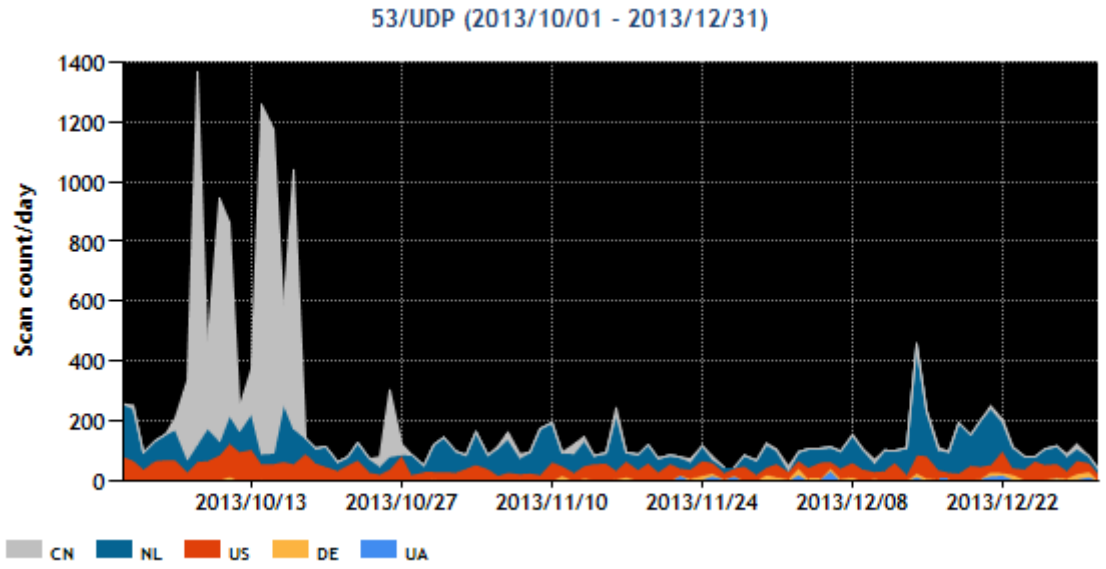
[図 4 2013 年 10～12 月の 123/UDP 宛のパケット観測数]

管理下のサーバやネットワーク機器などで NTP サーバの稼働状況を確認し、攻撃に使用されないよう適切な対策 (アップデート、パッチ、設定の変更など) を実施してください。

2.3 53/UDP 宛へのパケットの減少

前四半期の定点観測レポートで増加を報告した 53/UDP 宛のパケット数が 10 月中旬以降減少しました。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パケットが観測されなくなりました。これは、中国の通信事業者に割り当てられた IP アドレスへの DNS Amp 攻撃が終息したためと思われます。

ただし、中国の通信事業者に割り当てられた IP アドレス以外を送信元とするパケットが、少数ながら受信され続けています。オープンリゾルバの状態の DNS サーバを探索する活動が継続しているものと推測されます。



[図 5 2013 年 10～12 月の 53/UDP 宛のパケット観測数]

DNS Amp 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

NTP Project
DRDoS / Amplification Attack using ntpdc monlist command (*2)
http://support.ntp.org/bin/view/Main/SecurityNotice#DRDoS_Amplification_Attack_using

Hackers Spend Christmas Break Launching Large Scale NTP-Reflection Attacks (*2)
http://www.symantec.com/connect/blogs/hackers-spend-christmas-break-launching-large-scale-ntp-reflection-attacks

NTP reflection attack (*2)
https://isc.sans.edu/diary/NTP+reflection+attack/17300

CVE-2013-5211 (*2)
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5211