JPCERT CC®

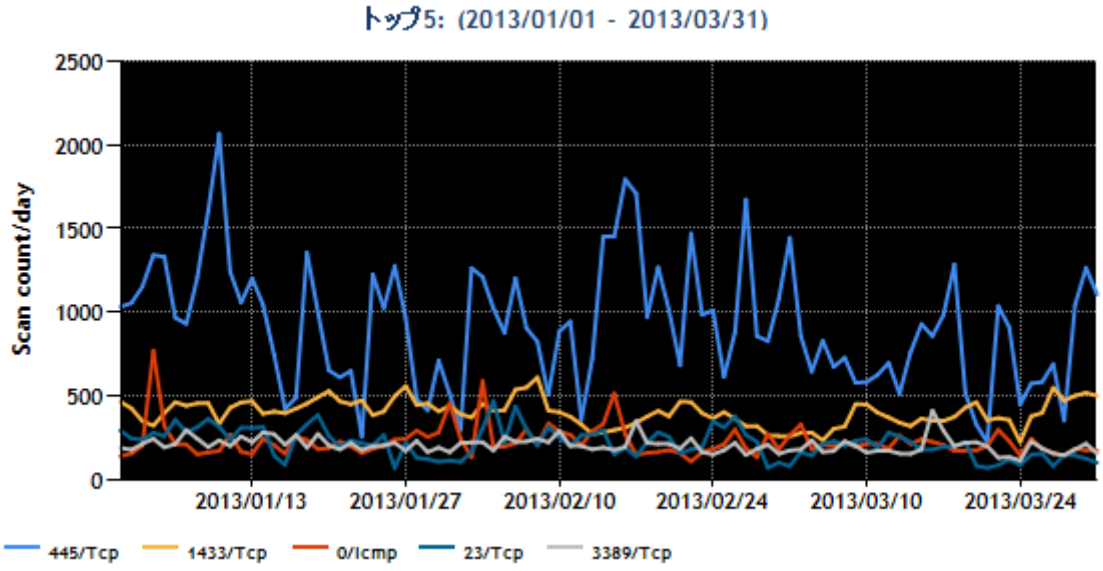
発行日 2013 年 4 月 25 日

JPCERT/CC インターネット定点観測レポート
[2013 年 1 月 1 日～3 月 31 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。脆弱性情報、マルウエアや攻撃ツールの情報などを参考に分析することで、攻撃活動や準備活動の捕捉に努めています。

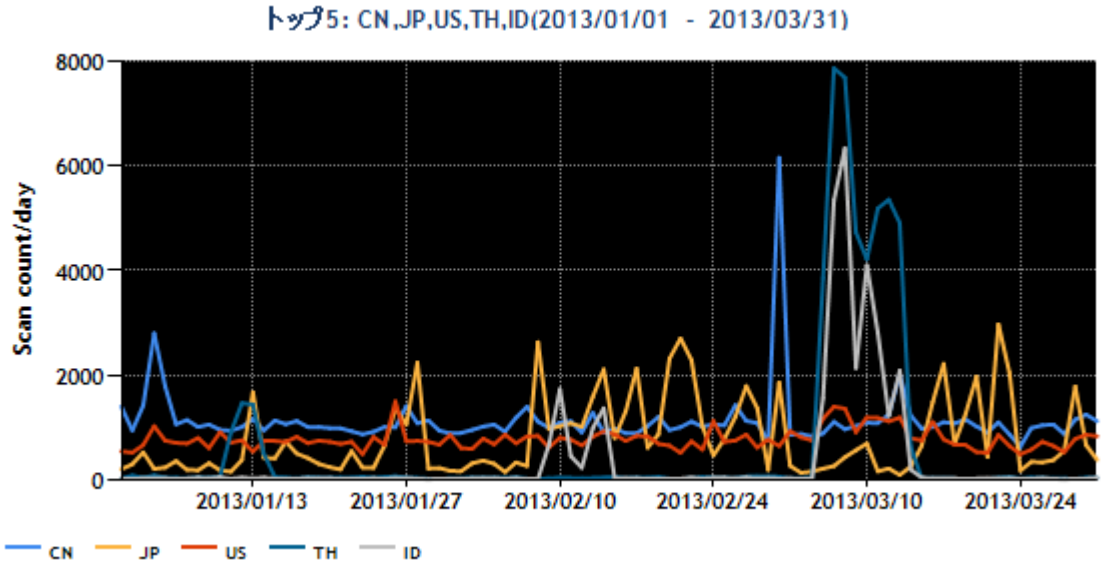
図 1 は期間中の宛先ポート番号トップ 5 の変化を示したグラフです。今期は、Windows や Windows Server 上で動作するプログラムが使用する 445/TCP や 1433/TCP、エラー通知や通信状態の診断を行なうための ICMP(Ping)、Telnet サーバが使用する 23/TCP、Windows のリモート管理やアクセスに使用するリモートデスクトップ 3389/TCP 宛へのパケットを多く観測しています。また、トップ 5 に続くものでは、22/TCP や、MySQL が使用する 3306/TCP、Web サーバで使用する 80/TCP 宛へのパケットなどを観測しています。



[図 1　2013 年 1~3 月の宛先ポート番号別パケット観測数トップ 5]

図 2 は期間中のパケット送信元地域トップ 5 の変化を示したグラフです。TOP5 の順位は、中国、日本、米国、タイ、インドネシアとなっています。トップ 5 の中では、日本国内から特定センサーの 21318/TCP 宛へのスキャンが急増したことにより前四半期 3 位だった日本が 2 位へ、2 位だった

米国が 3 位へと順位が入れ替わっています。

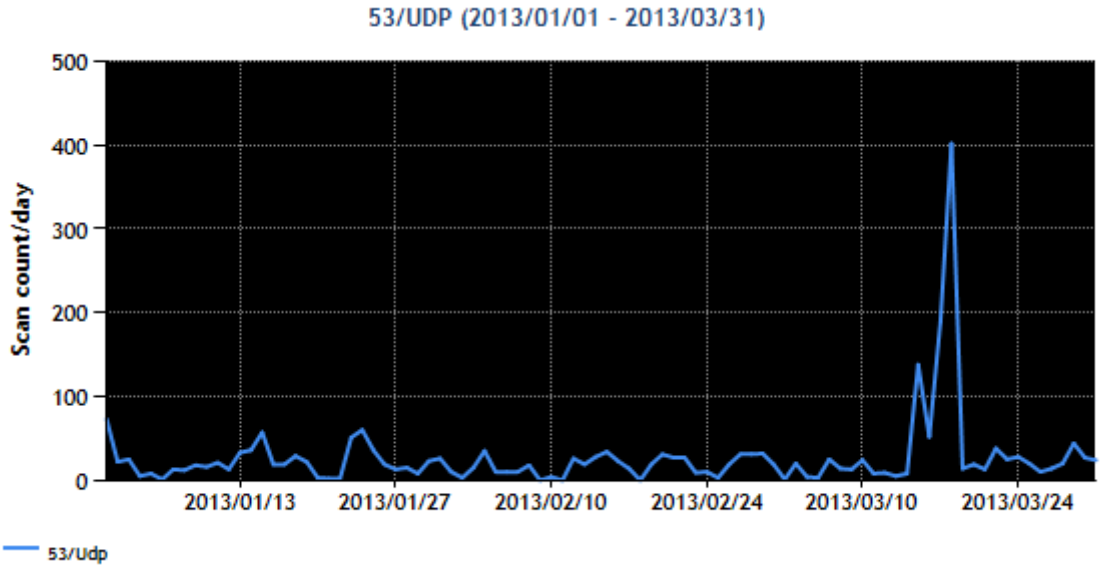


[図 2　2013 年 1~3 月の送信元地域別トップ 5]

2　注目された現象

2.1　53/UDP 宛のパケットの観測

期間中の宛先ポート番号のトップ 5 には含まれていませんが、本四半期に、53/UDP 宛のパケットの一時的な増加が観測されました。図 3 は 53/UDP 宛のパケットの変化を示したグラフです。



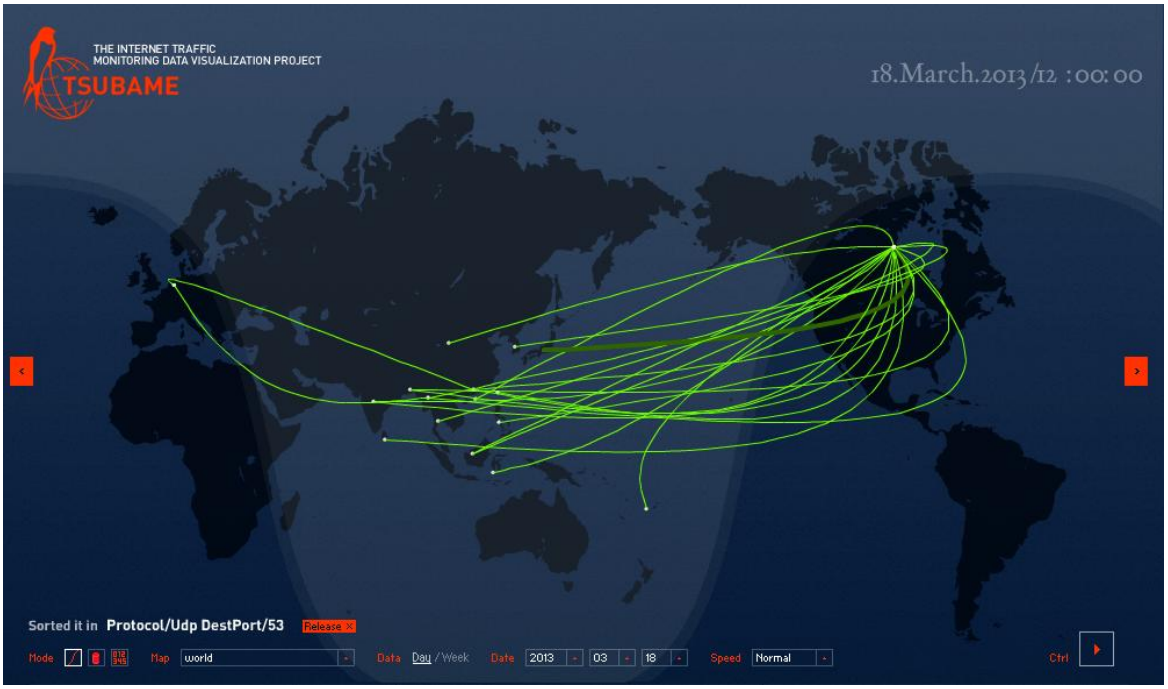
[図 3　2013 年 1~3 月の 53/UDP 宛のパケット観測数]

3 月 15 日から 3 月 19 日までの間、53/UDP 宛のパケットが急増しました。複数の報道等が取り上げた、欧州を中心に活動する非営利のスパム対策組織の Spamhaus Project と、米セキュリティ企業である Cloudflare 社のサーバに対する、DNS サーバを使用したサイバー攻撃 (DDoS 攻撃) に関連していると思われます。

DNS サーバへの問合せパケットは、通常は正規の DNS サーバに 1 パケットが送られるだけですが、今回の事例では、同じ送信元 IP アドレスをもつ 53/UDP 宛のパケットを短時間に多数のセンサーが受信しています。これは、DNS サーバが小さな問合せパケットに対して比較的大きな応答パケットを返すことが多い特性を使った DDoS 攻撃 (DNS Amp といいます。詳細は以下の URL を参照してください。) の一端が観測されたものだと推測しています。

株式会社日本レジストリサービス(JPRS)
DDoS にあなたの DNS が使われる ～DNS Amp の脅威と対策～
http://jprs.jp/related-info/guide/003.pdf

3 月 15 日から 3 月 19 日までの間にセンサーで確認したパケットの送信元地域は、カナダが最も多く、続いてオランダ、米国の順となっています。



[図 4　2013 年 3 月 18 日の 53/UDP 宛のパケット送信イメージ]

図 4 はアジア・太平洋地域に設置されている TSUBAME プロジェクトのセンサーが観測した 53/UDP 宛のパケットの流れを可視化した図です。図 4 では、カナダとオランダの 2 つの地域から、日本を初めとするアジア・太平洋地域の各センサーに対して 53/UDP 宛のパケットが送られている様子が

見てとれます。実際には、送信元 IP アドレスが詐称された 53/UDP 宛のパケットがもっと広範囲に送られていると考えられます。仮にセンサーが置かれた IP アドレスに応答する DNS サーバがあれば、大きなサイズの応答パケットが詐称された送信元 IP アドレスに送られて通信負荷を押し上げます。すなわち、詐称された送信元の IP アドレスをもつノードが、攻撃対象として狙われているのです。

参考文書：

US-CERT Alert (TA13-088A)
DNS Amplification Attacks
http://www.us-cert.gov/ncas/alerts/TA13-088A

Internet Systems Consortium
Is Your Open DNS Resolver Part of a Criminal Conspiracy?
https://www.isc.org/wordpress/is-your-open-dns-resolver-part-of-a-criminal-conspiracy/

TrendMicro
DNS Amp 手法による過去最大規模の DDoS 攻撃、スパム対策組織「Spamhaus」がターゲットに
http://blog.trendmicro.co.jp/archives/7012

IBM Tokyo SOC Report
Spamhaus に対する DNS リフレクション攻撃について
https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/dnsreflection?lang=ja