発行日 ：2012-10-23

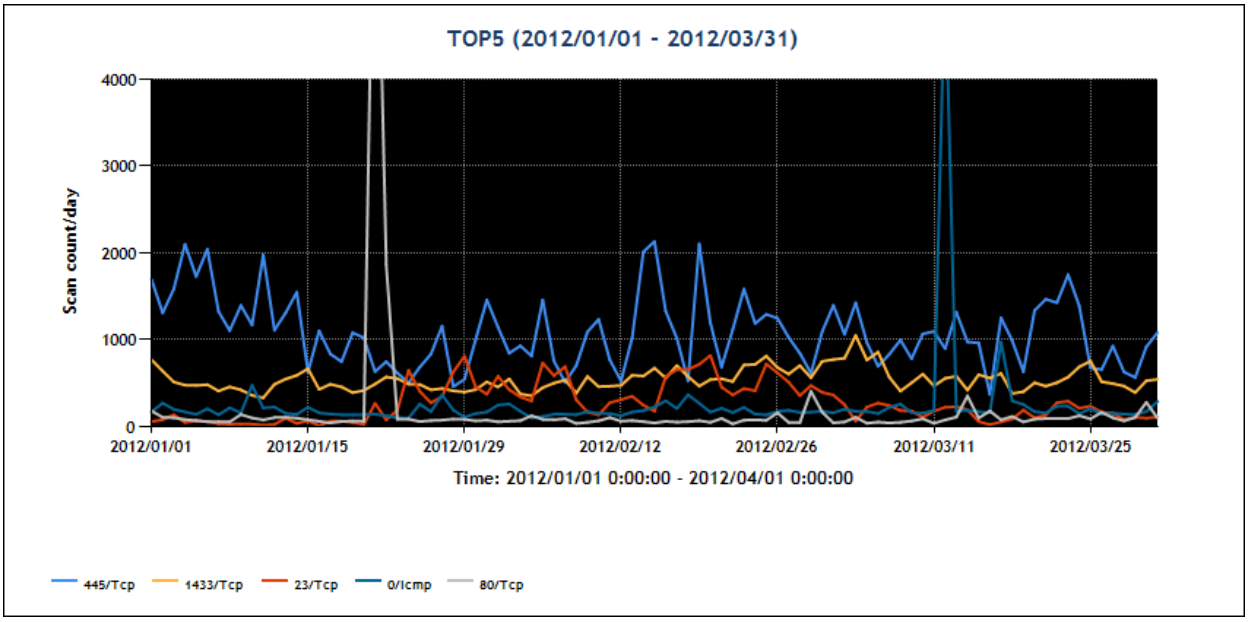
JPCERT/CC インターネット定点観測レポート[2012 年 1 月 1 日～3 月 31 日]

1 概況

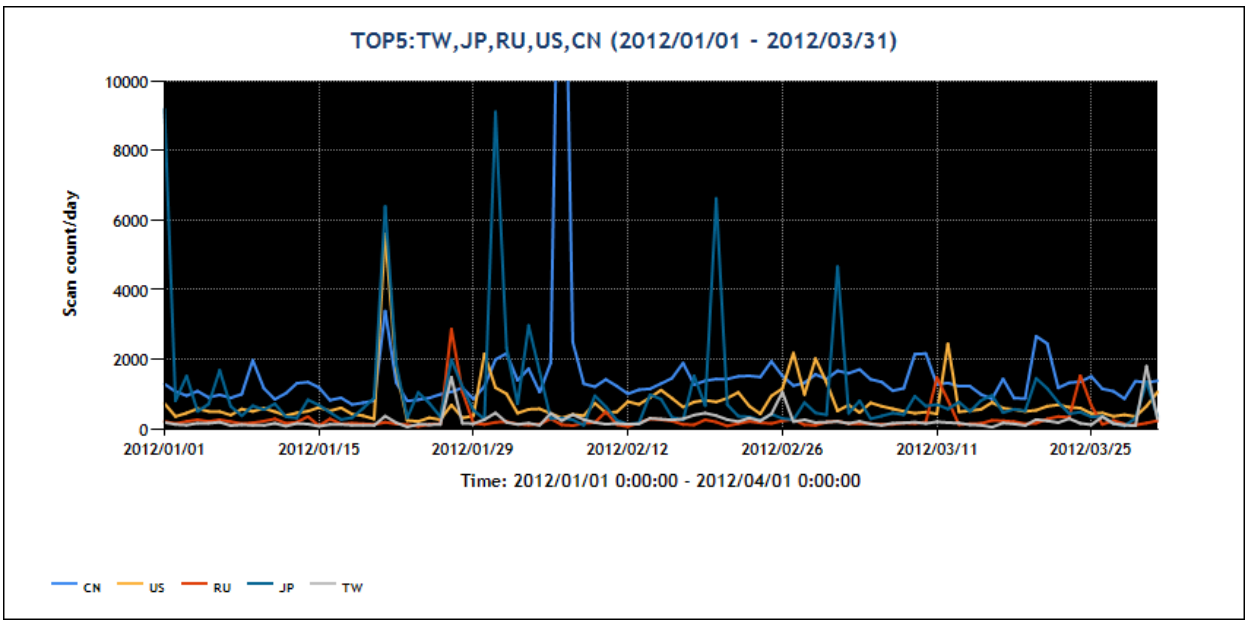
JPCERT/CC では、インターネット上に複数のセンサーを分散配置し、不特定多数に向けて発信されるパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類しています。脆弱性情報、マルウエアや攻撃ツールの情報などの情報を参考に分析することで、攻撃活動や準備活動の補足に努めています。

図 1 は期間中の宛先ポート番号 TOP5 の変化を示したものです。今期は、Windows や、サーバ上で動作するプログラムが使用する 445/TCP や 1433/TCP 宛へのパケットが多く観測されています。また、UNIX/Linux のリモートアクセスで広く使われている 23/TCP 宛のパケット数に大きな増減が見られました。この件については、「2. 注目された現象」に記載しています。

図 2 は期間中のパケット送信元地域 TOP5 の変化を示したものです。センサーの観測状況では、中国を送信元地域としたパケットが多数観測されています。また、日本国内の特定の IP からの短時間に特定のセンサーに対し多数のパケットが届くという事象が数回発生しています。同 IP からのパケットは他のセンサーでは観測されていません。発生理由は不明ですが、サービスの稼働状況の把握を目的としたスキャンではないと思われ、影響は無いと考えます。



[図 1　2012 年 1~3 月の宛先ポート番号別パケット観測数 Top5]



[図 2　2012 年 1~3 月の送信元地域別 Top5]

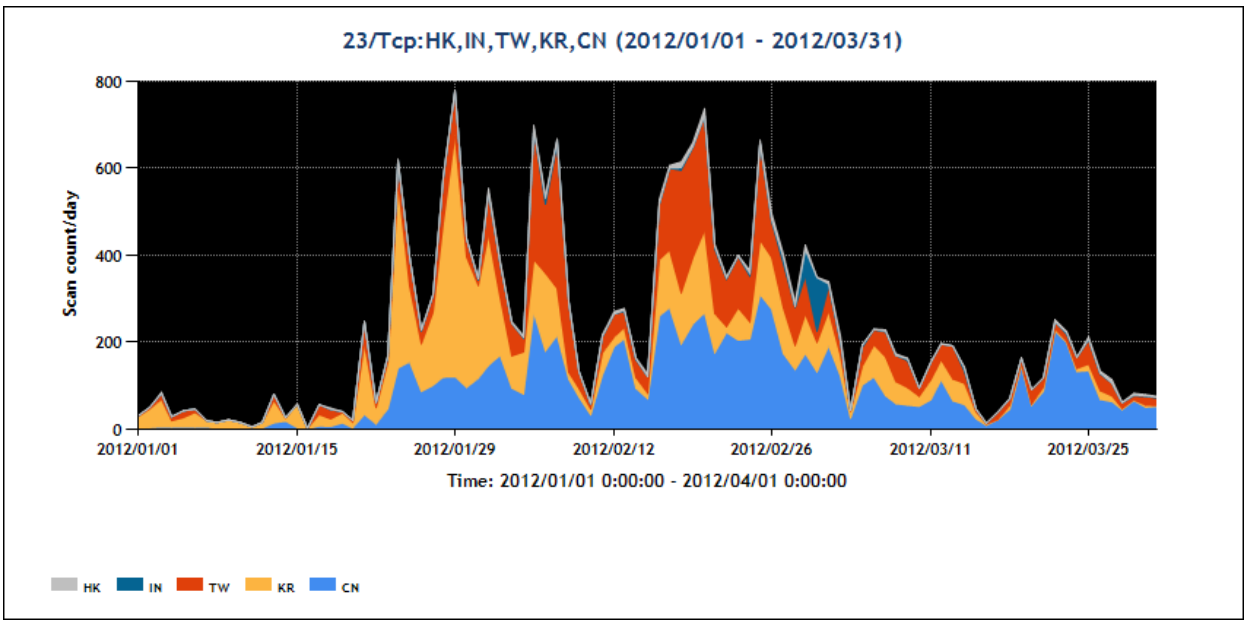
2　注目された現象

2.1　23/TCP 宛のパケットの増減

23/TCP を宛先ポートとしたパケットは、2011 年 12 月上旬から変動を繰り返しながらも増加した状態が続いています。発信元が複数の地域に渡っている点も、図 3 の通り今期も変わりがありません。

これらのパケットは、Telnet を待ち受けるサーバを組み込んだ機器を対象としたパケットと思われます。送信元のノードは、VoIP アダプタや Web カメラなどのネットワーク機器であり、23/TCP 宛にパケットを送る必然性がありません。

これらのネットワーク機器はマルウエアに感染しており、マルウエアが感染したネットワーク機器から、第三者に対して攻撃者が指示したアドレスレンジに対してパケットを送信していると考えられます。



[図 3　2012 年 1~3 月の 23/TCP 宛のパケット観測数]