発行日 ：2012-10-23

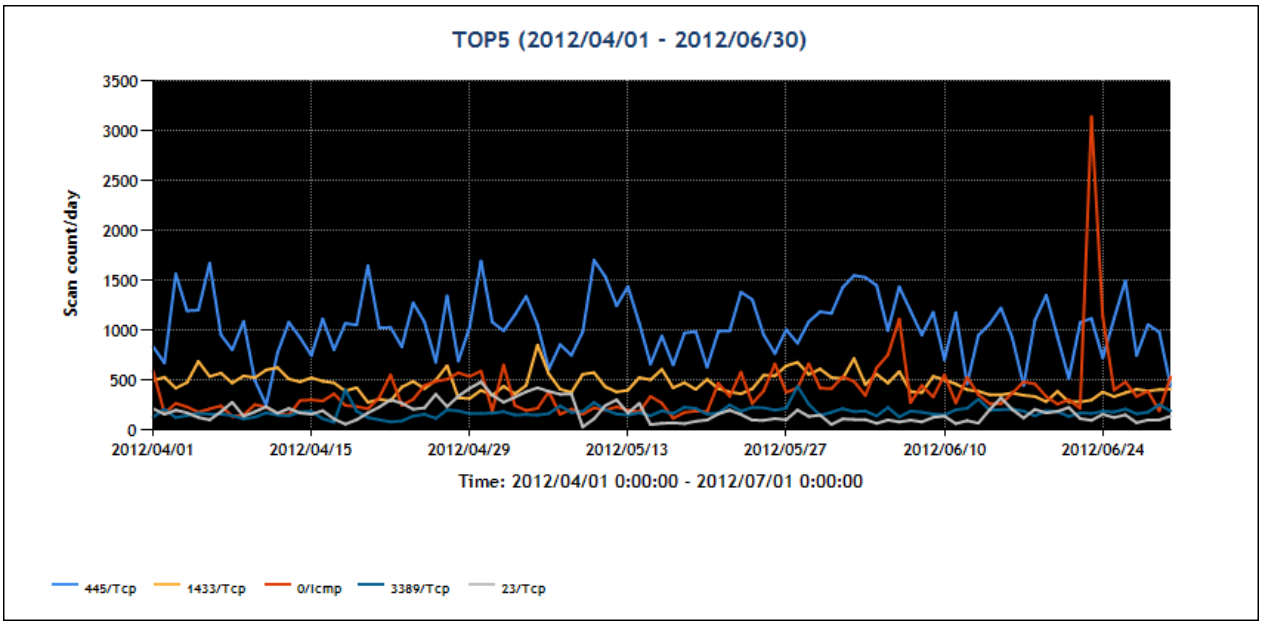
JPCERT/CC インターネット定点観測レポート[2012 年 4 月 1 日～6 月 30 日]

1 概況

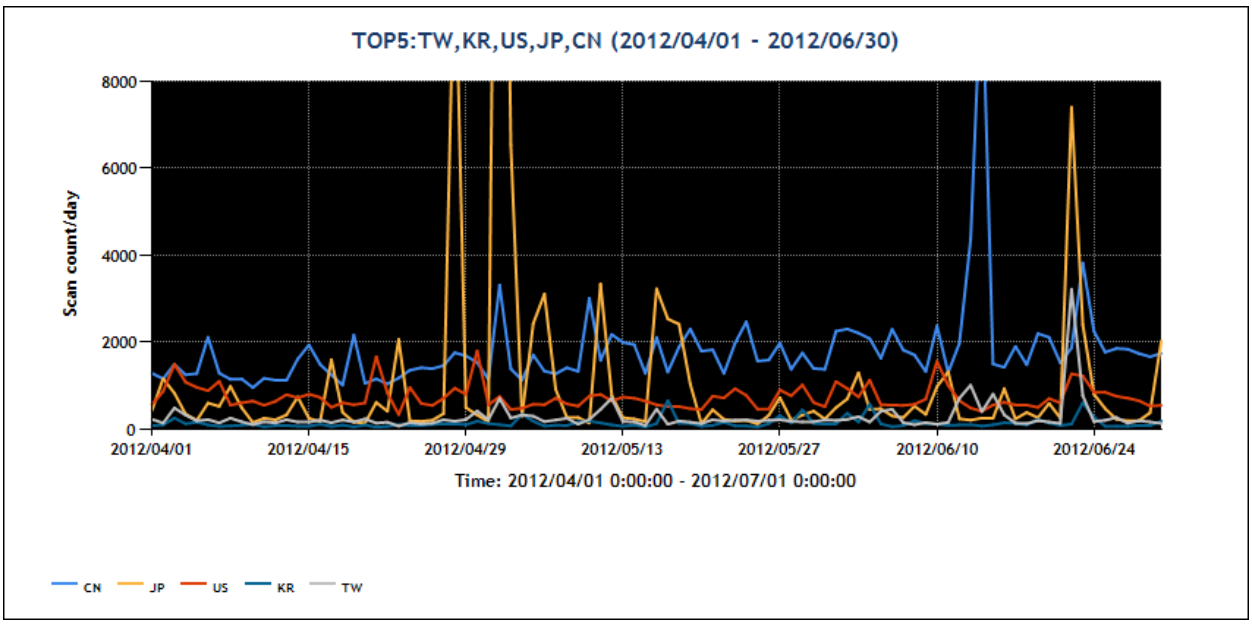
JPCERT/CC では、インターネット上に複数のセンサーを分散配置し、不特定多数に向けて発信されるパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類しています。脆弱性情報、マルウエアや攻撃ツールの情報などを参考に分析することで、攻撃活動や準備活動の補足に努めています。

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、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 宛へのパケットが多く観測されています。また、Linux のリモートアクセスで広く使われている 22/TCP や、23/TCP 宛のパケットは、Windows を対象としたパケット数と比較すると数は減りますが、TOP10 の間に含まれています。

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ました。また、送信元地域が中国と推測されるパケットの多くは、複数のポート番号に対して同一発信元から短時間に連続してパケット送信される特徴が見られました。



[図 1　2012 年 4~6 月の宛先ポート番号別パケット観測数 Top5]



[図 2　2012 年 4~6 月の送信元地域別 Top5]

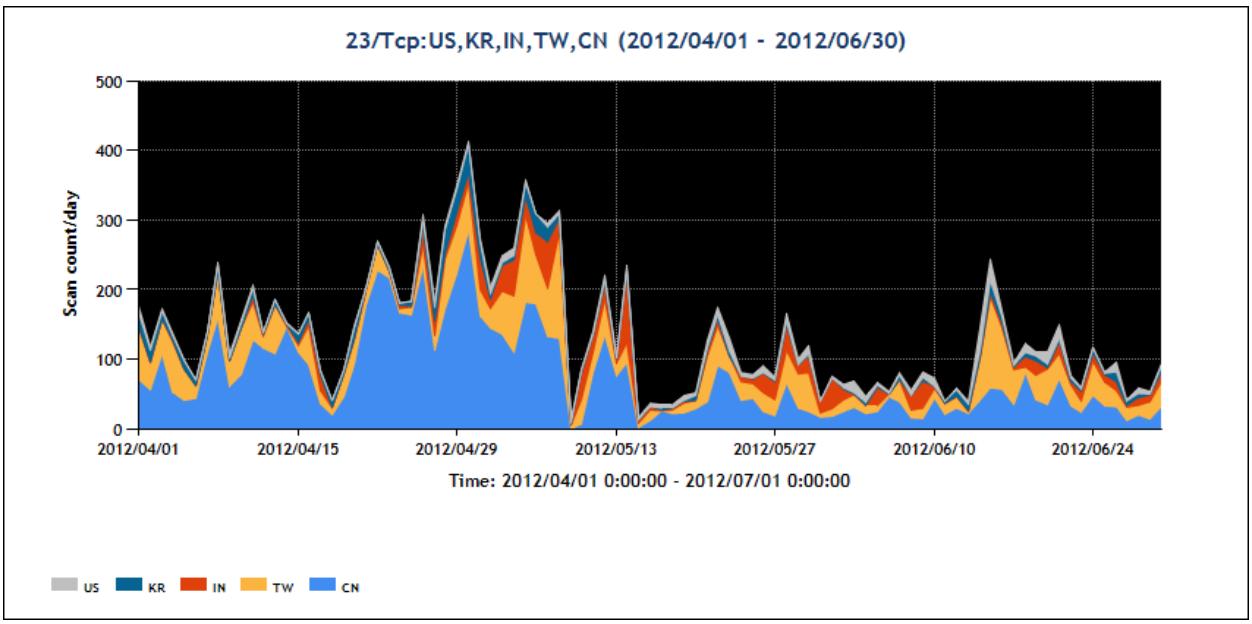
2　注目された現象

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ています。今期は図 3 のとおり増減を繰り返しつつ、韓国や中国、台湾などの地域からパケットが観測されています。

これは、Telnet を待ち受けるサーバを搭載した組込機器を対象としたパケットと思われます。そうした製品が国外では少なからず使用されているようです。送信元 IP アドレスでは、Web カメラやルータなどのネットワーク機器が動作しています。機器本来の目的からすると、23/TCP 宛にパケットを送る必要はありません。

攻撃者は該当 IP アドレスで動作するネットワーク機器を攻略しマルウエアに感染させ、管理下に置きます。機器利用者は、意図せず第三者に対してパケットを送信していると考えられます。

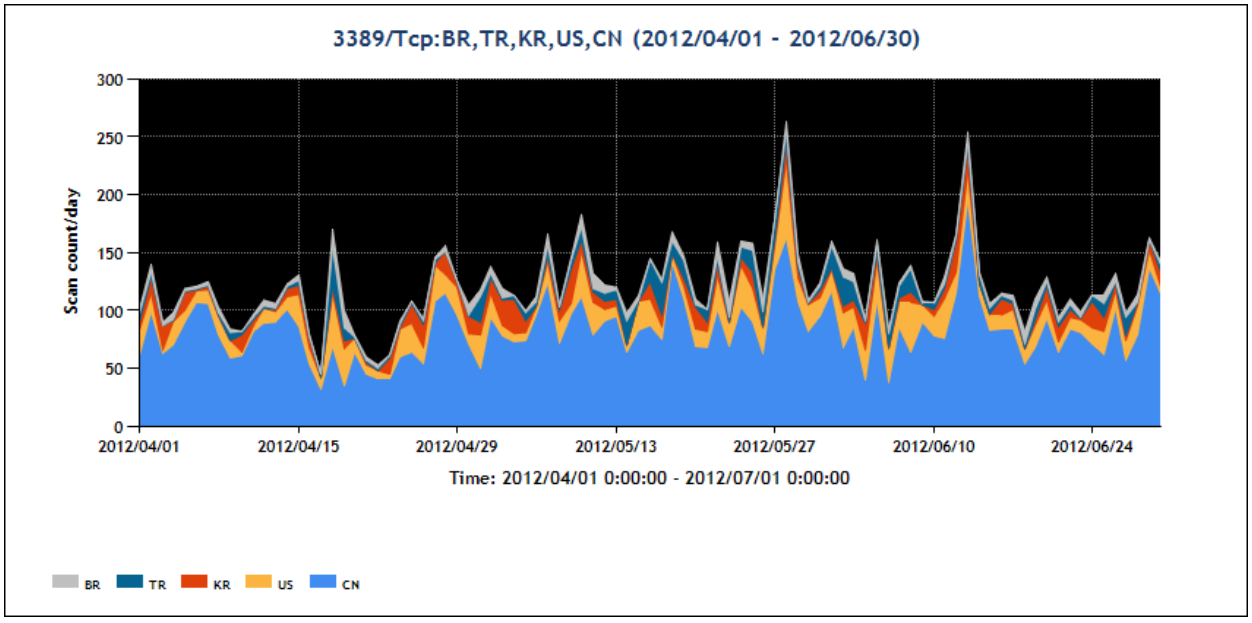


[図 3　2012 年 4~6 月の 23/TCP 宛のパケット観測数]

2.2　3389/TCP 宛のパケットの増加

3389/TCP を宛先ポートとしたパケットは、2011 年 7 月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。今期は図 4 の通り、5 月 1 日頃から増加した状態が続いています。

3389/TCP 宛へのパケットの観測数は、マルウエア Morto とその亜種に関する情報公開日前後で変動が見られます。センサーの 3389/TCP 宛にパケットを送信した IP アドレス上で、未知のマルウエアがスキャン活動をしていた事例も確認されました。



[図 4　2012 年 4~6 月 3389/TCP 宛のパケット観測数]