JPCERT CC®

発行日：2013 年 3 月 6 日

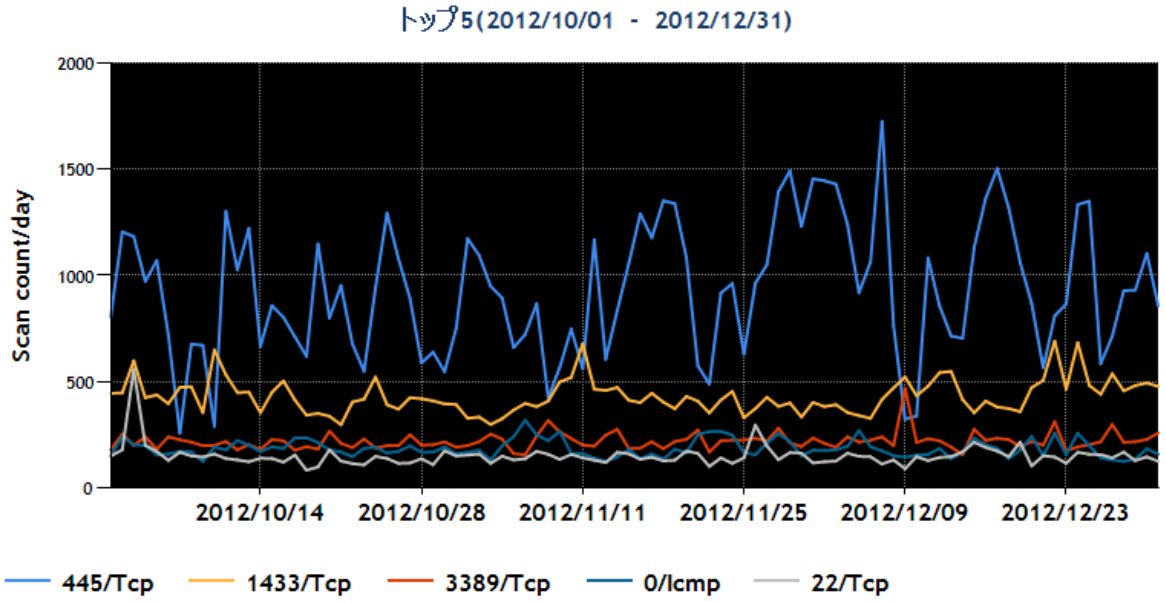
JPCERT/CC インターネット定点観測レポート
[2012 年 10 月 1 日～12 月 31 日]

1 概況

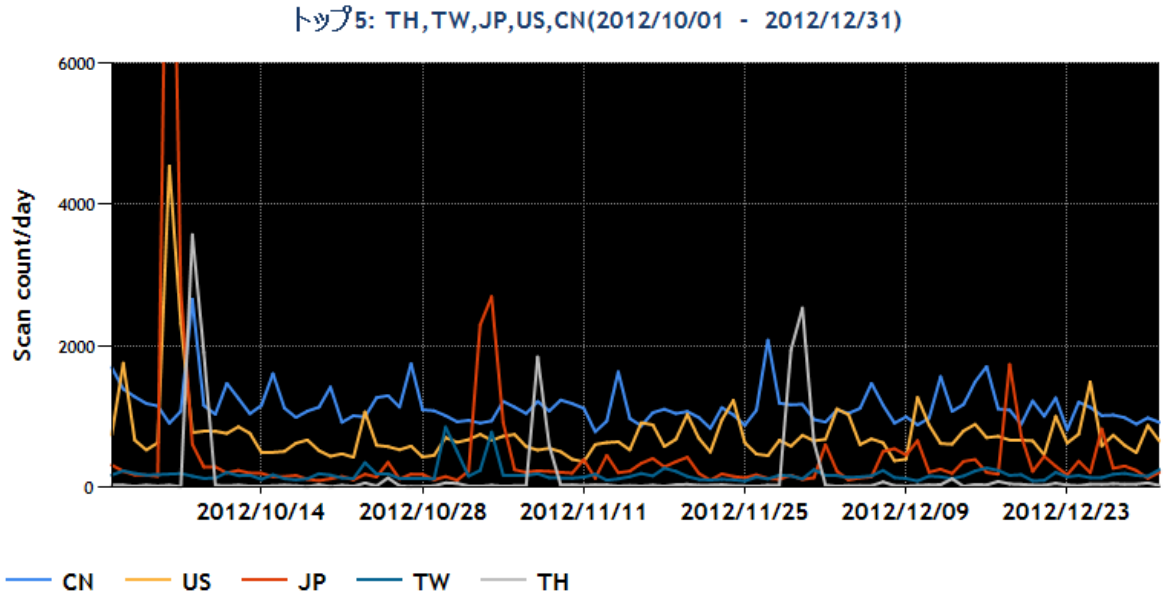
JPCERT/CC では、インターネット上に複数のセンサーを分散配置し、不特定多数に向けて発信されるパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類しています。脆弱性情報、マルウエアや攻撃ツールの情報などを参考に分析することで、攻撃活動や準備活動の捕捉に努めています。

図 1 は期間中もっとも多く観測された 5 位までの宛先ポート番号(以下トップ 5 と記す)をもった観測パケット数の変化を示したものです。今四半期は、22/TCP の宛先ポート番号をもつパケット数が増加し、23/TCP に替わり 5 番目になりました。これについては「2. 注目された現象」で取り上げます。

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、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、Windows を対象としたパケットが多く占めるトップ 5 に対し、続くトップ 10 には 22/TCP や、23/TCP 宛など主に Linux を対象としたパケットが並んでいました。
図 2 は期間中のパケット送信元地域トップ 5 の変化を示したものです。トップ 5 ではロシアの順位が下がり、ランク外となっています。これは 445/TCP を宛先としたパケットが減少したためです。代わりに、23/TCP 宛のパケットが増加したため、タイがトップ 5 にランクインしています。タイからは Windows を対象としたパケットが多く観測されています。



[図 1　2012 年 10~12 月の宛先ポート番号別パケット観測数トップ 5]

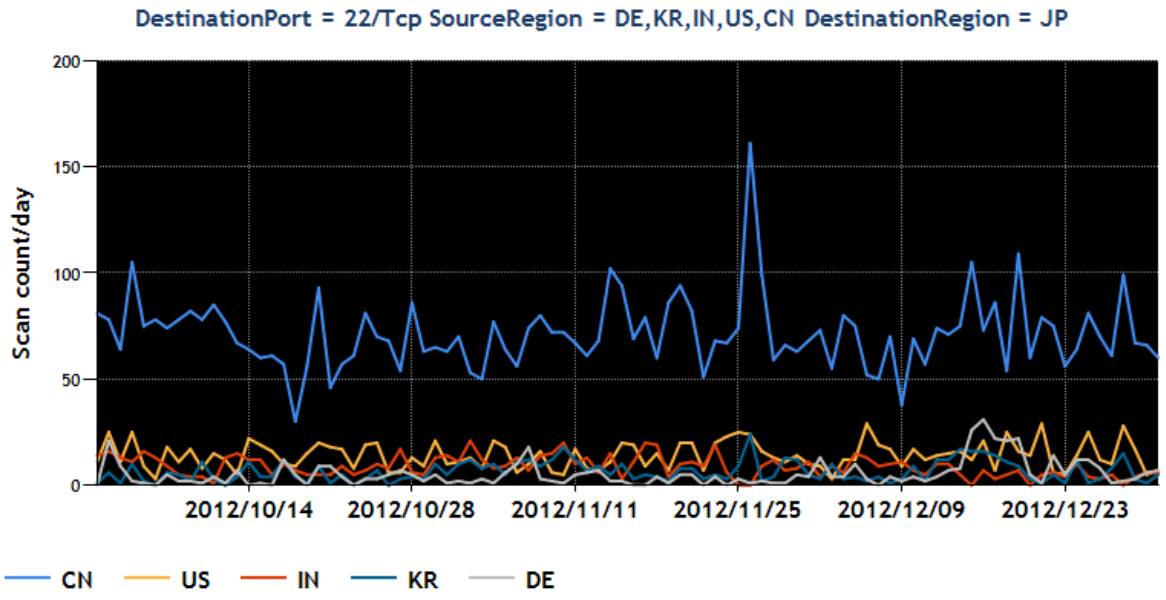


[図 2　2012 年 10~12 月の送信元地域別トップ 5]

2　注目された現象

2.1　22/TCP 宛のパケットの増減

22/TCP 宛のパケットは、図 1 のグラフのように今期宛先ポート番号別で 5 番目に多くパケットを観測しました。図 3 は 22/TCP 宛パケットの送信元地域トップ 5 の変化を示したものです。米国や中国、インドなどの地域から観測しています。送信元地域のトップ 5 には含まれていませんが、国内の複数の IP アドレスを送信元としたパケットも観測されました。



[図 3　2012 年 10~12 月の 22/TCP 宛のパケット観測数]

22/TCP 宛のパケットは、主に同ポート番号で待ち受けていることが多い、SSH サーバを探索するためのスキャンと思われます。弊センターでは、22/TCP 宛のパケットを送信していた IP アドレスの管理者に対し連絡を行いました。その結果、複数の IP アドレスの管理者から頂いた情報によると、問題のパケットの発信元サーバは、第三者に遠隔からログインされた形跡があり、新たな 22/TCP 宛のパケットを送信し SSH サーバの発見、および ID とパスワードのアカウントを調査するためのツールが動作していました。

攻撃者は、事前に作成した辞書ファイルを情報を使用し、該当する ID とパスワードを使用している SSH サーバを探索し、ログイン可能なサーバを新たな攻撃活動に使用しているものと思われます。