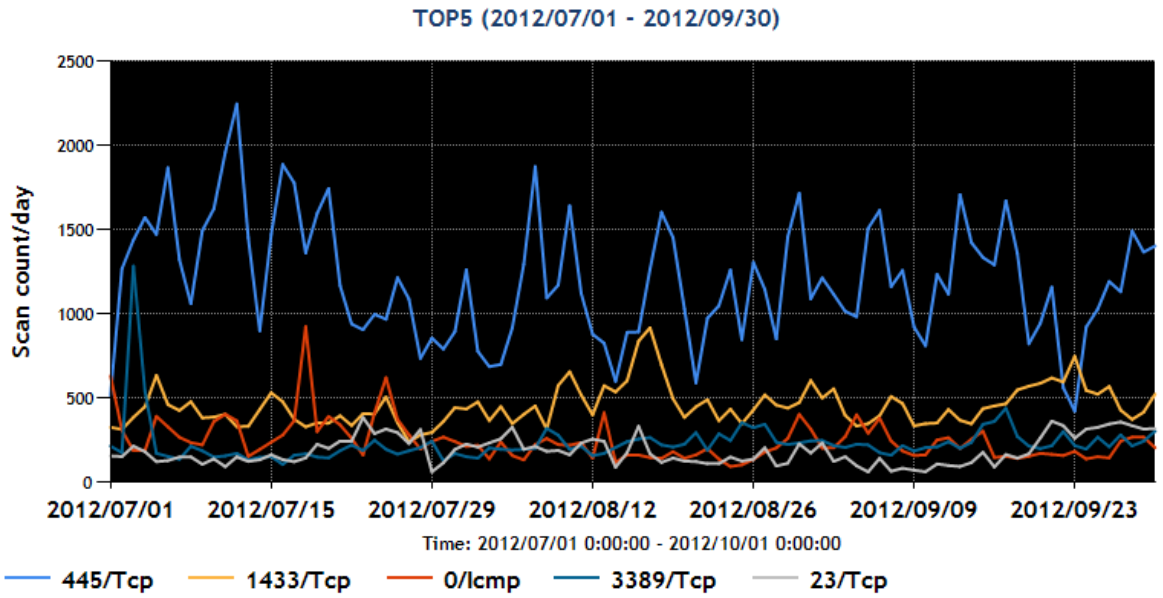
発行日：2012 年 12 月 19 日

JPCERT/CC インターネット定点観測レポート
[2012 年 7 月 1 日～9 月 30 日)

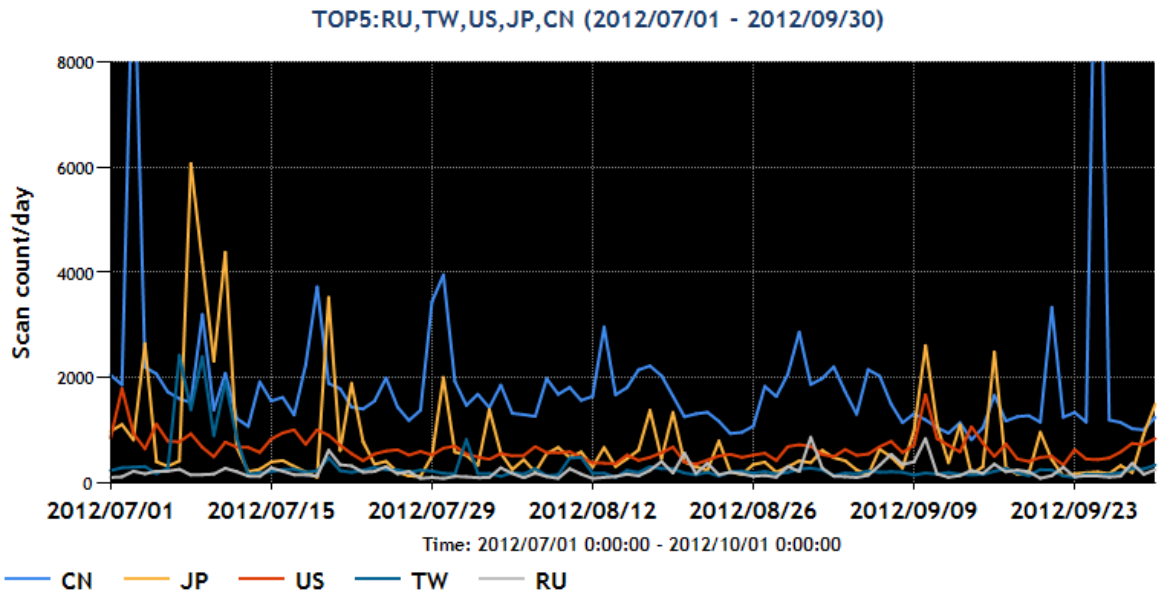
1 概況

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捕捉に努めています。

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。Top5 の順位に変化はありませんでした。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た Top5 に対し、続く Top10 までには 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。TOP5 では韓国の順位が下がり、ランク外となっています。これは 445/TCP を対象としたパケットが減少したためです。代わりに台湾が、23/TCP 宛のパケットが増加したため、TOP5 にランクインしています。台湾からの 23/TCP のパケットは、PC ではなくなんらかの NW 機器が感染して発信していると思われます。



[図 1　2012 年 7~9 月の宛先ポート番号別パケット観測数 Top5]

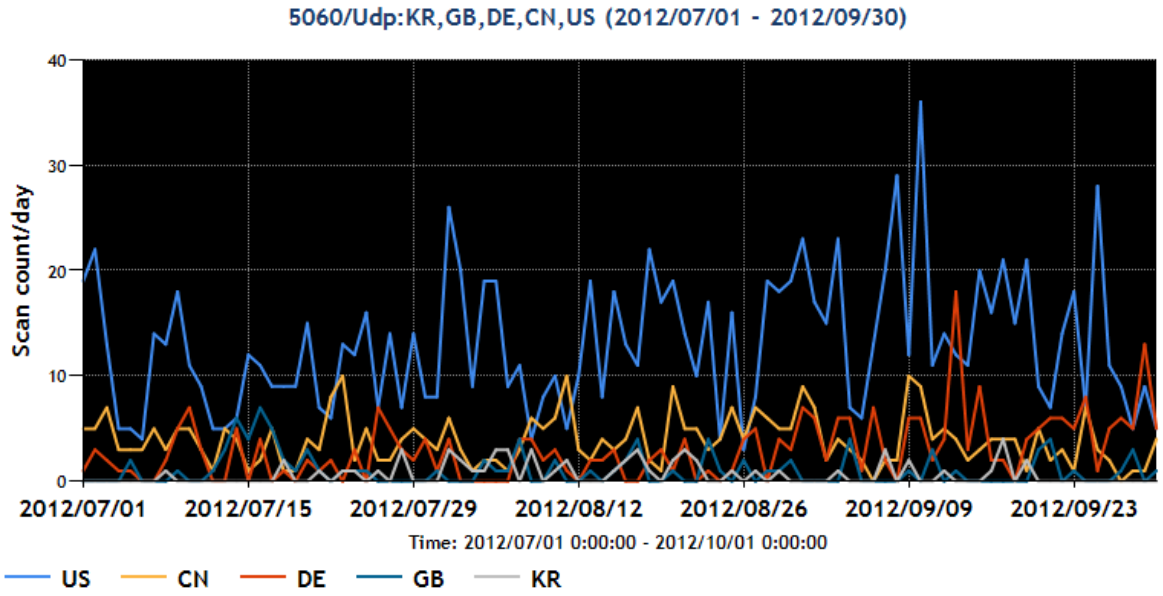


[図 2　2012 年 7~9 月の送信元地域別 Top5]

2　注目された現象

2.1　5060/Udp 宛のパケットの増減

5060/UDP 宛のパケットは、期間中の宛先ポート番号 TOP5 には含まれませんでしたが、注目しておきたいと思います。図 3 はパケット送信元地域 TOP5 の変化を示したものです。米国や中国、ドイツなどの地域から 5060/Udp 宛のパケットが観測されました。送信元地域 TOP5 には含まれていませんが、国内の複数の IP アドレスを送信元地域としたパケットも観測されました。

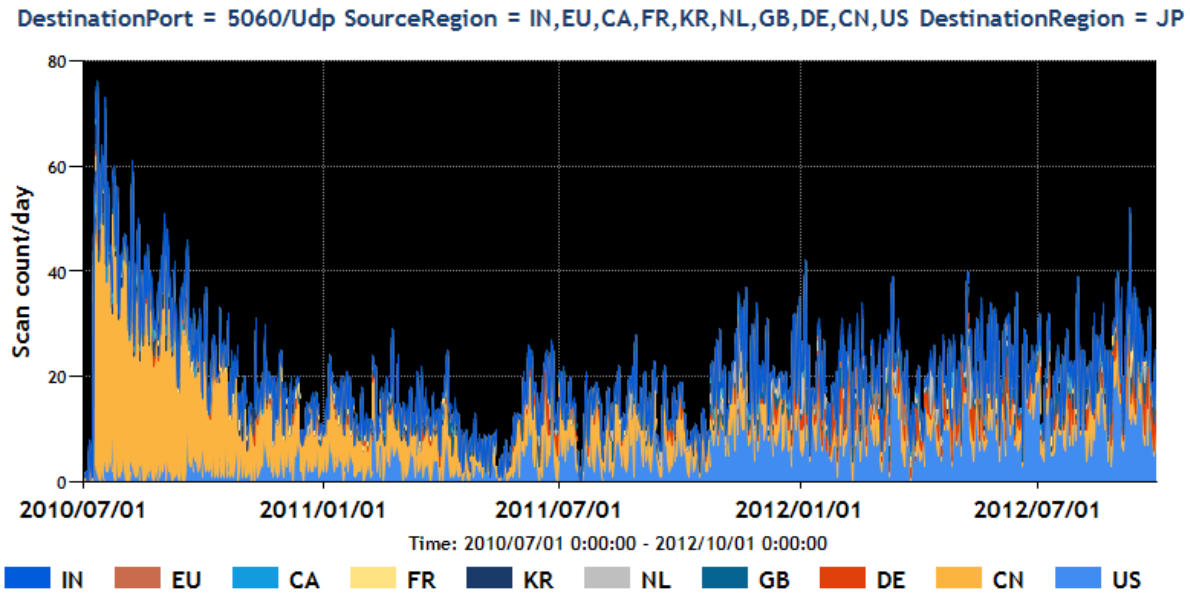


[図 3　2012 年 7~9 月の 5060/UDP 宛のパケット観測数]

5060/UDP を対象としたパケットは、主に SIP サーバを探索するためのスキャンと思われますが、その中に送信時に使用するポート番号やパケット内の文字列にツール名を含んだ特徴的なパケットがあります。

これらのパケットは、インターネット上に公開されている SIP サーバの探索と、脆弱な ID とパスワードの SIP アカウントを調査することが目的と思われます。また、これらのパケットは攻撃者によって攻略されたサーバ上にツールが設置され、踏み台サーバがパケット送信が行わっている事例が複数確認しました。

このような攻撃は、2010 年 7 月上旬に急増しその後減少はしましたが、継続して観測されています。今期と過去の状況比較のために長期のグラフを作成し、図 4 に示します。
今期は数は少ないですが、日本国内の複数の IP アドレスが加わるなど、送信元 IP アドレス数が増加していることから攻撃拠点が増加していると考えられます。



[図 4　2010 年 7 月~2012 年 9 月の 5060/UDP 宛のパケット観測数]

参考文書：

主に UNIX / Linux 系サーバを対象としたインターネット公開サーバのセキュリティ設定に関する注意喚起に関する注意喚起
https://www.jpcert.or.jp/at/2011/at110002.html