JPCERT CC®

Japan Computer Emergency
Response Team Coordination Center

JPCERT-IA-2017-02

発行日 ：2017-05-11

JPCERT/CC インターネット定点観測レポート
[2017 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観測用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、これを脆弱性情報、マルウエアや攻撃ツールの情報などと対比して分析することで、攻撃活動や準備活動の捕捉に努めています。なお、本レポートでは、本四半期に観測された日本宛のパケットを中心に分析した結果について述べます。

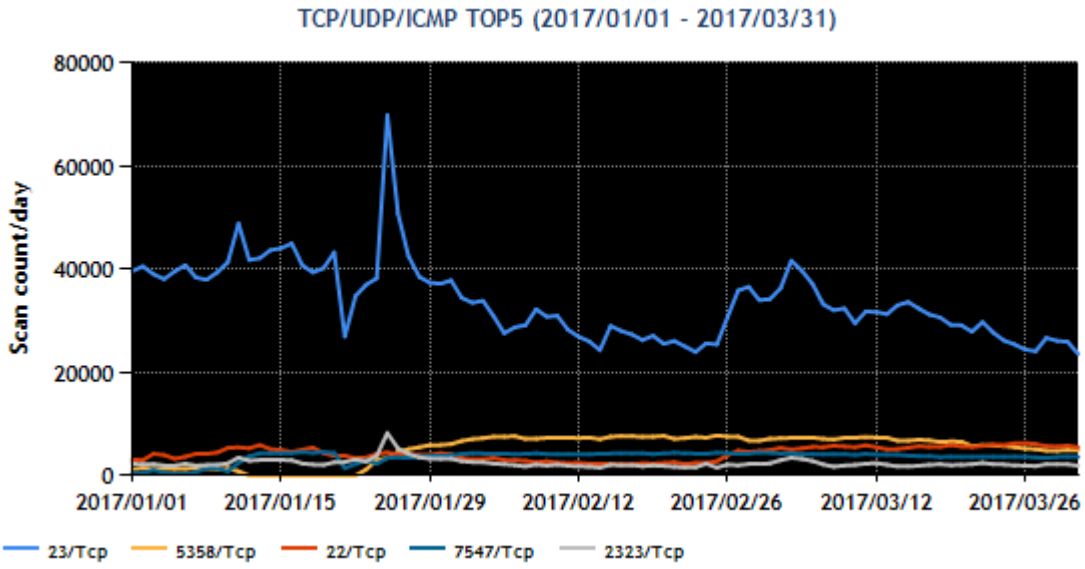
宛先ポート番号別パケット観測数のトップ 5 を［表 1］に示します。

［表 1：宛先ポート番号トップ 5］

順位	宛先ポート番号	前四半期の順位
1	23/TCP (telnet)	1
2	5358/TCP	トップ 11 以下
3	22/TCP (ssh)	4
4	7547/TCP	3
5	2323/TCP	2

※ポート番号とサービスの対応の詳細は、IANA の文書(*1)を参照してください。なお、サービス名は IANA の情報をもとに記載していますが、必ずしも各サービスプロトコルに則ったパケットが受信されているとは限りません。

図 1 は、期間中のトップ 5 の宛先ポート番号ごとのパケット観測数の推移を示しています。



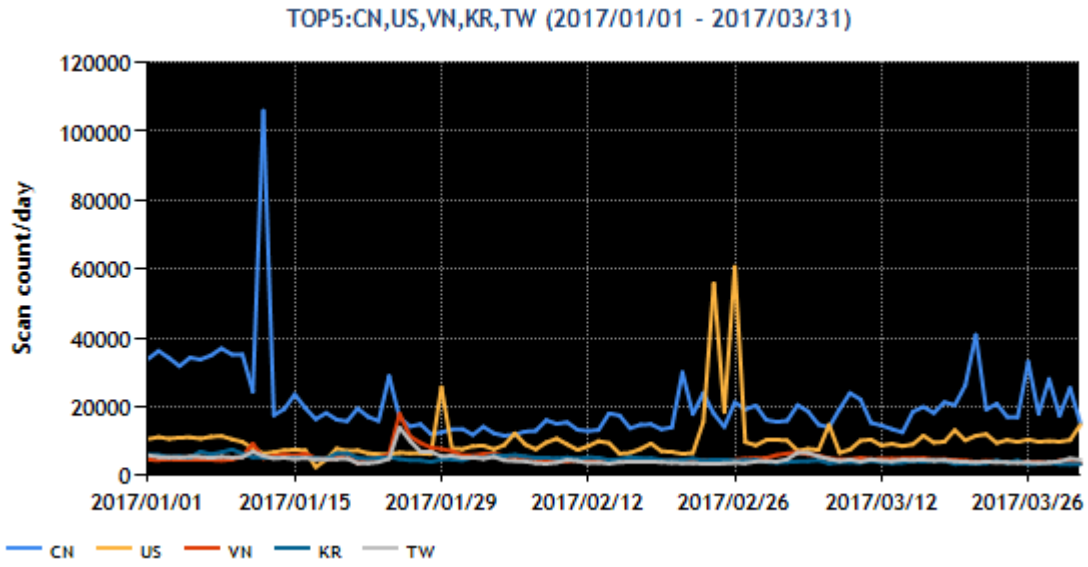
［図 1：2017 年 1～3 月の宛先ポート番号別パケット観測数トップ 5 の推移］

送信元地域のトップ 5 を［表 2］に示します。

［表 2：送信元地域トップ 5］

順位	送信元地域	前四半期の順位
1	中国	1
2	米国	2
3	ベトナム	4
4	韓国	5
5	台湾	3

図 2 に期間中のトップ 5 のパケット送信元地域からのパケット観測数の推移を示します。



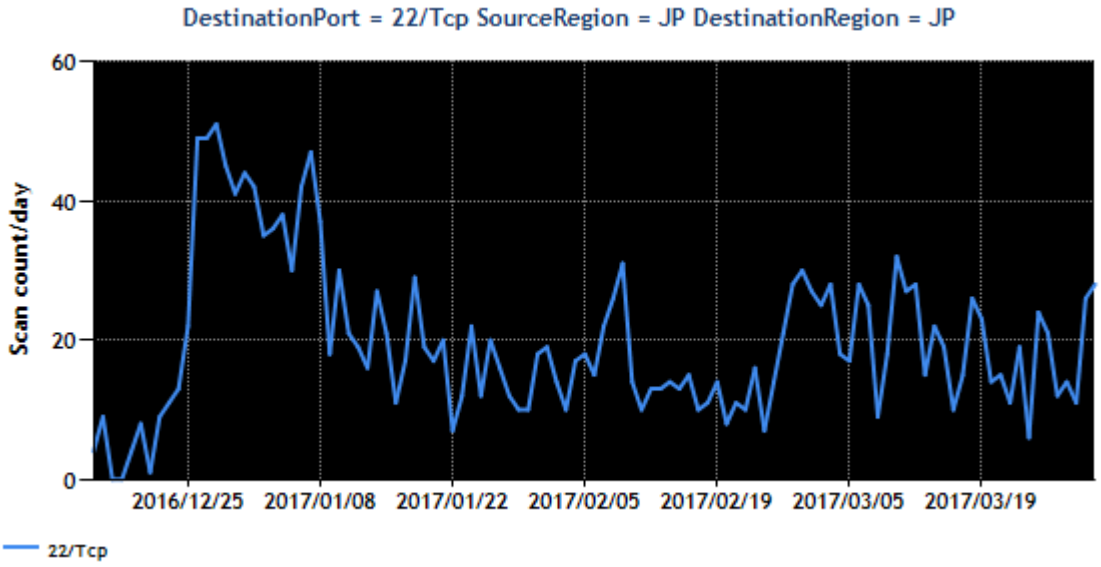
［図 2：2017 年 1～3 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

本四半期は、ある程度普及している機器がリクエストを待ち受けていると思われる 22/TCP や 23/TCP 等のポートに対するパケットが、主な地域において、従来よりも多く観測されました。この傾向はベトナムと韓国において特に顕著で、送信元地域別のトップ 5 における両地域の順位が一つずつ上がる結果となりました。なお、多く観測されるようになったパケットの宛先ポートごとの割合は、送信元地域によらず、ほぼ同じでした。その他に関しては、特筆すべき状況の変化は見られませんでした。

2　注目された現象

2.1　Port22/TCP 宛のパケット数の増加

国内の IP アドレスから SSH サーバが使用するポートに対するパケットが 2016 年 12 月 25 日頃より増加し、その後も増減はありますが継続して観測されています。（図 3）

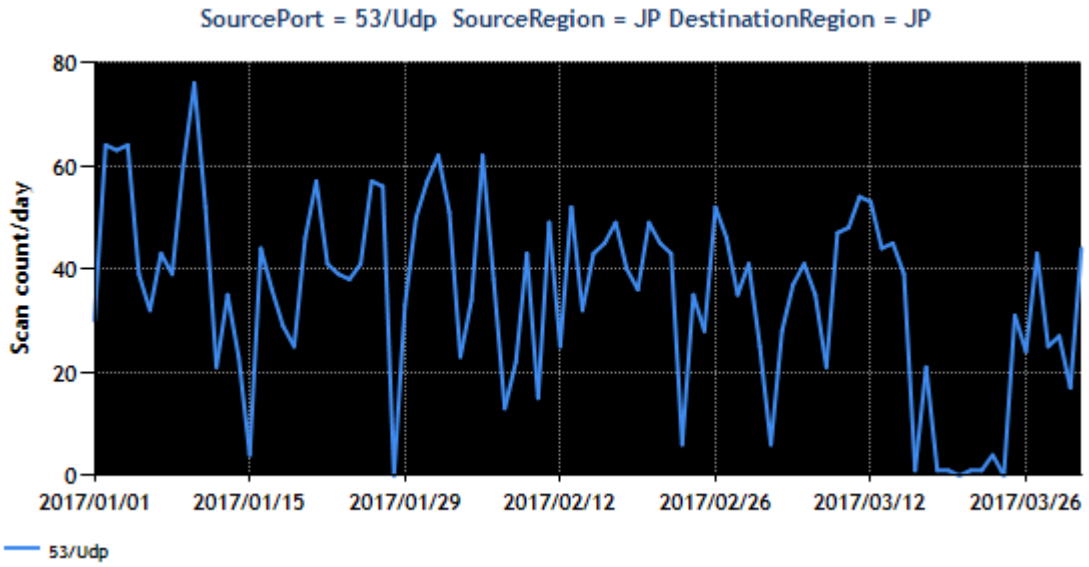


［図 3：Port22/TCP 宛のパケットのトップ 10 ごとのパケット観測数の推移］

これらのパケットから無作為に複数個を抽出し送信元について確認を行ったところ、約半分が複数の海外ベンダ製の NAS と推測されました。
これらの NAS 製品はユーザが Web サーバ、Telnet、SSH 等のサービスを追加機能として設定できる製品であり、因果関係については判明しておりませんが、ユーザが追加した機能がマルウエアによる攻撃を受け、NAS 製品がマルウエアに感染したためパケットを送信しているのではないかと推測される事例を確認しています。
Web サーバが稼働しているサーバには、フィッシングサイトへの誘導を目的としたリダイレクト用の HTML コンテンツが置かれた事例も確認しています。
遠隔の第三者がアクセス可能な Telnet や SSH 等のサービスが意図せず稼働していないか、アクセスログの確認等もあわせて行うことをおすすめします。

2.2 国内のオープンリゾルバ等を使った DNS 水責め攻撃

本四半期も、DNS のクエリに対するリプライパケットを国内外の多数の IP アドレスから受信しました。受信したパケットを分析したところ、存在しないランダムなホスト名の名前解決要求パケットに対する応答パケットであることが分かりました。これは、DNS 水責め攻撃のために、TSUBAME のセンサーの IP アドレスを詐称して、オープンリゾルバに送信された名前解決要求パケットに対する応答パケットと考えられます。送信元 Port53/UDP からのパケット数の推移を図 4 に示します。



［図 4. 53/UDP からのパケット観測数の推移］

オープンリゾルバは、影響が深刻な攻撃手法である DNS 水責め攻撃を支える土壌の一つになっていると考えられますので、JPCERT/CC ではオープンリゾルバをもつ組織の管理者に情報を提供して改善を求める活動を継続して行っています。一部の管理者からはオープンリゾルバであるかを調査した結果、ルータのファームウエアアップデート、フィルタルール設定などの対策を行った旨の返信をいただきました。

JPCERT/CC では引き続き、オープンリゾルバを減らすべく努力していく予定です。

3 参考文献

(1) Service Name and Transport Protocol Port Number Registry
https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

本活動は、経済産業省より委託を受け、「平成 28 年度サイバー攻撃等国際連携対応調整事業」として実施したものです。