Japan Computer Emergency Response Team Coordination Center

JPCERT-IA-2016-03
発行日 : 2016-11-16

JPCERT/CC インターネット定点観測レポート
[2016 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。

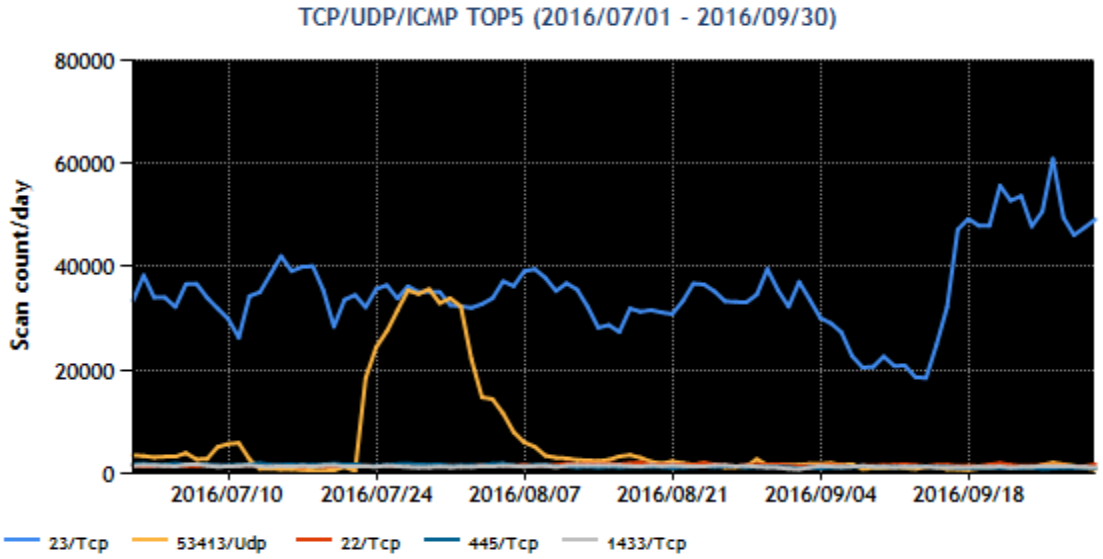
宛先ポート番号別パケット観測数のトップ 5 を［表 1］に示します。

［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	53413/UDP	2
3	22/TCP	6
4	445/TCP (microsoft-ds)	5
5	1433/TCP (ms-sql-s)	3

※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。



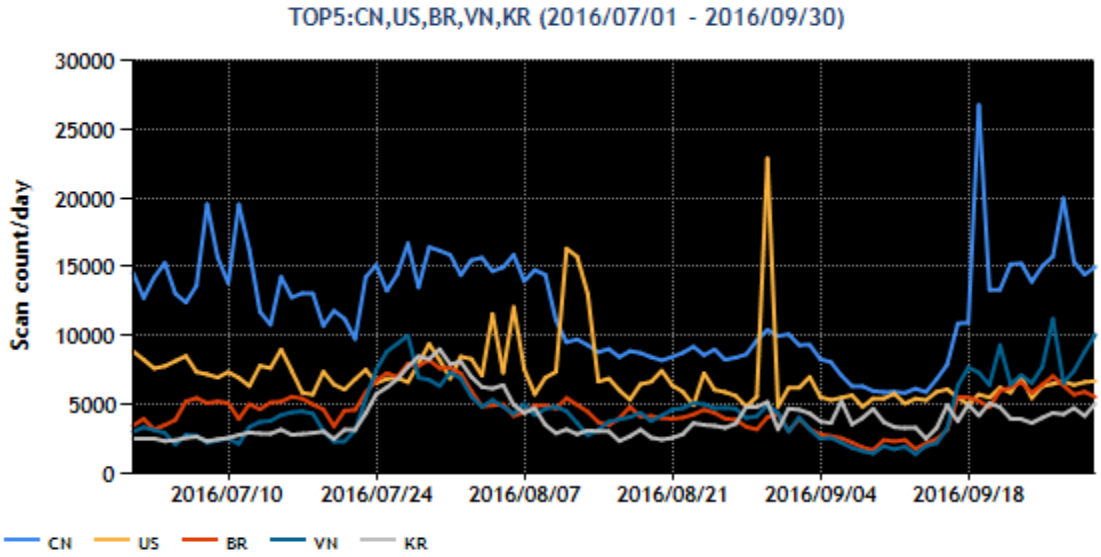
［図 1：2016 年 7～9 月の宛先ポート番号別パケット観測数トップ 5 の推移］

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	ブラジル	3
4	ベトナム	7
5	韓国	5

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。



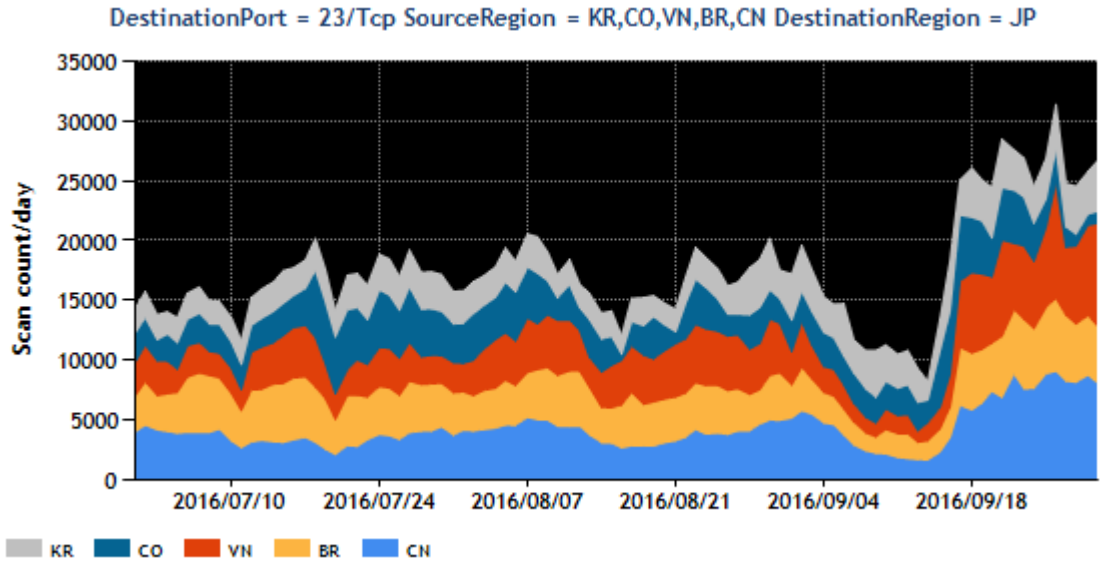
［図 2：2016 年 7～9 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

本四半期は、23/TCP 宛のパケットが 9 月 15 日前後に急増しました。この現象については、「2.1 Port23/TCP 宛のパケット数の増加」で詳しく述べます。また、Port53413/UDP 宛のパケットの受信数が 7 月 23 日から約 2 週間増えた状態が続きました。この現象の要因については、過去の類似現象と同様に海外製のルータを対象とした探索や攻撃活動と思われます。その他の宛先ポート番号のトップ 5 については、特筆すべき内容はありません。次に、送信元地域別のトップ 5 では、ベトナムが前四半期の 7 番目から 4 番目になりました。ベトナムが TOP5 に入った理由は、宛先ポート番号別の内訳で一番多く 5 割強を占めた 23/TCP 宛のパケットのおよそ 1 割がベトナムを送信元地域としていたためです。その他の地域については、多少の増減はありましたが、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　Port23/TCP 宛のパケット数の増加

2016 年 9 月 17 日ごろから Port23/TCP 宛のパケット数が増加しています。特定の 1 地域を送信元地域とするパケットだけが増えたのではなく、複数の地域からのパケットが増加しました（図 3）。なお、Port23/TCP や Port2323/TCP の探索と思われるパケットが増加し、Telnet が動作しているサイトにログインを試みるマルウエア mirai の活動が盛んになったとの@police からのレポート(*2)も、TSUBAME の観測結果と同じ現象を報告しているものと思われます。



［図 3. Port23/TCP 宛のパケット数の推移］

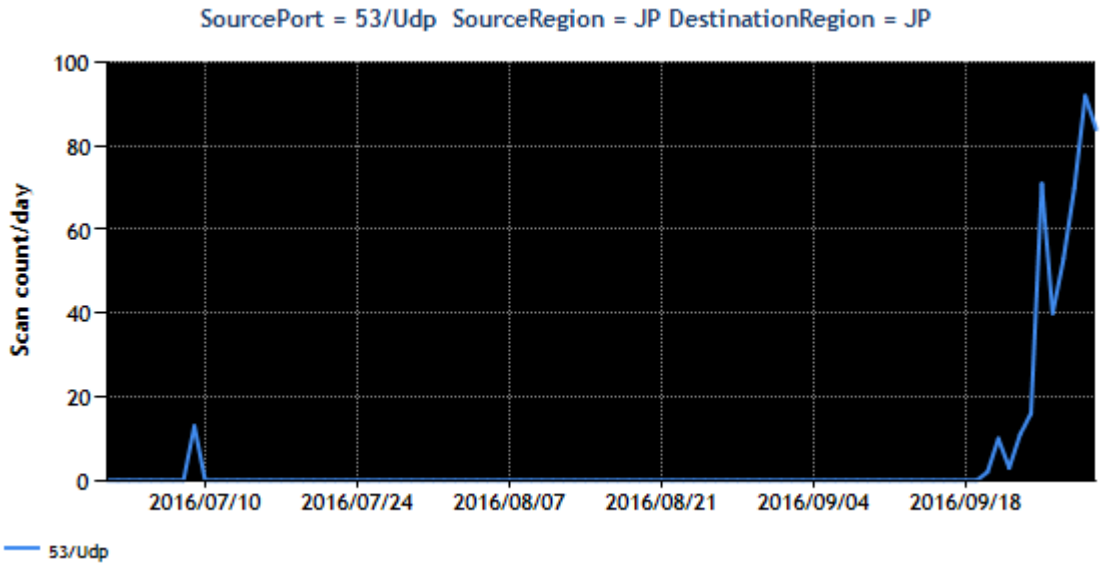
Port23/TCP 等を探索するパケットの送信元を調べると、特定の機種の製品が頻繁に見つかったり、特定の ISP が管理する IP アドレスを付与されていることが多かったりすることが分かります。前者は、製品の導入時の初期設定手順に問題がある場合が多く、後者は特定のネットワーク上に多数の機器を配備しているサービス提供事業者の問題によるものと推測されます
JPCERT/CC ではこれまでも不審なパケットを低減させるために、送信元 IP アドレスに設置されている機器を調査して機種を推定し、当該製品の改修を期待して製造ベンダ等に、また当該機器の利用者に設定の変更を促す通知を出してもらうことを期待して関連 ISP 等に、それぞれ情報を提供してきましたが、本四半期においては、後者の問題に対応するため、多数の監視カメラや特定産業向け組込み通信機器をネットワーク上に配備し保守管理を請け負っているベンダを次のような情報を手掛かりに特定し、適切な対処を求める活動を開始しました。

- 送信元 IP アドレスの Port80 等で動作する Web サーバのレスポンス
- Telnet、SSH 等のログイン要求時の文字列

本四半期は、それぞれ 1 社の機器の製造ベンダとサービス提供事業者に対して情報を提供しました。

2.2　国内のオープンリゾルバ等を使った DNS 水責め攻撃の再開

DNS のクエリに対するリプライパケットを TSUBAME が、国内外の多数の IP アドレスから受信しています。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］

9 月 20 日より、日本国内からオープンリゾルバ等を使った DNS 水責め攻撃が観測されるようになりました。DNS 水責め攻撃は 2014 年頃から頻繁に見られましたが、しばらく観測されない時期が続いていました。攻撃が再び観測されるようになった理由は不明です。オープンリゾルバ等を用いた DNS 水責め攻撃は影響が深刻な攻撃手法の一つと考えられますので、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善処を求める活動を再開しました。既に一部の管理者からは、ルータのフィルタルールの不備などの調査結果を含む返信をいただきました。

JPCERT/CC では引き続き、DNS 水責め攻撃を少しでも抑えられるよう、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
http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

(2) @police
インターネット観測結果等（平成 28 年 9 月期）
https://www.npa.go.jp/cyberpolice/detect/pdf/20161020.pdf

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。