JPCERT-IA-2016-02
発行日 : 2016-05-26

JPCERT/CC インターネット定点観測レポート
[2016 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。

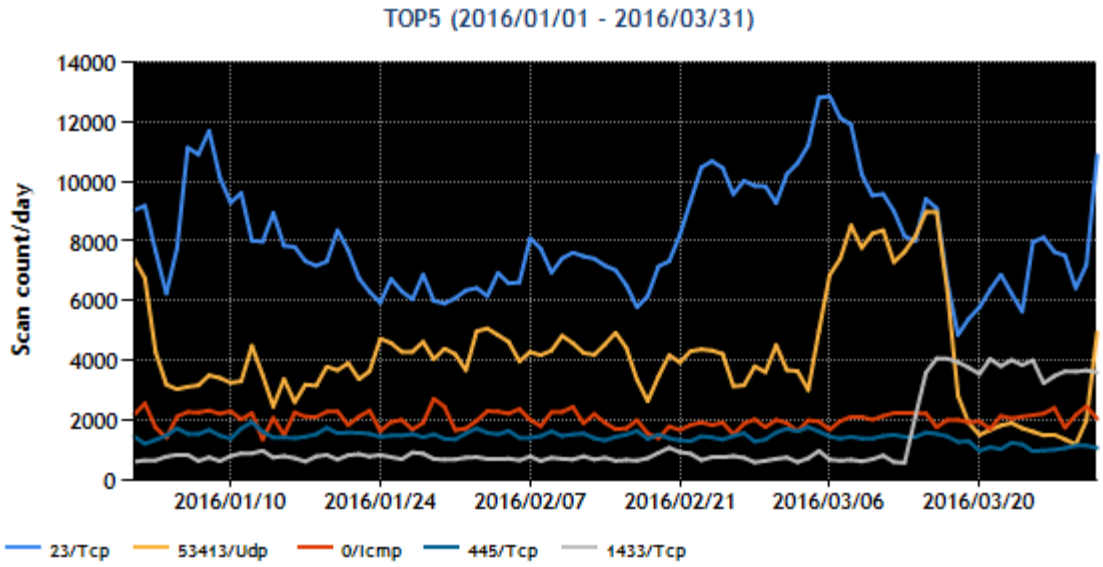
宛先ポート番号別パケット観測数のトップ 5 を [表 1]に示します。

[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	53413/UDP	3
3	0/ICMP	2
4	445/TCP (microsoft-ds)	4
5	1433/TCP (ms-sql-s)	5

※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。



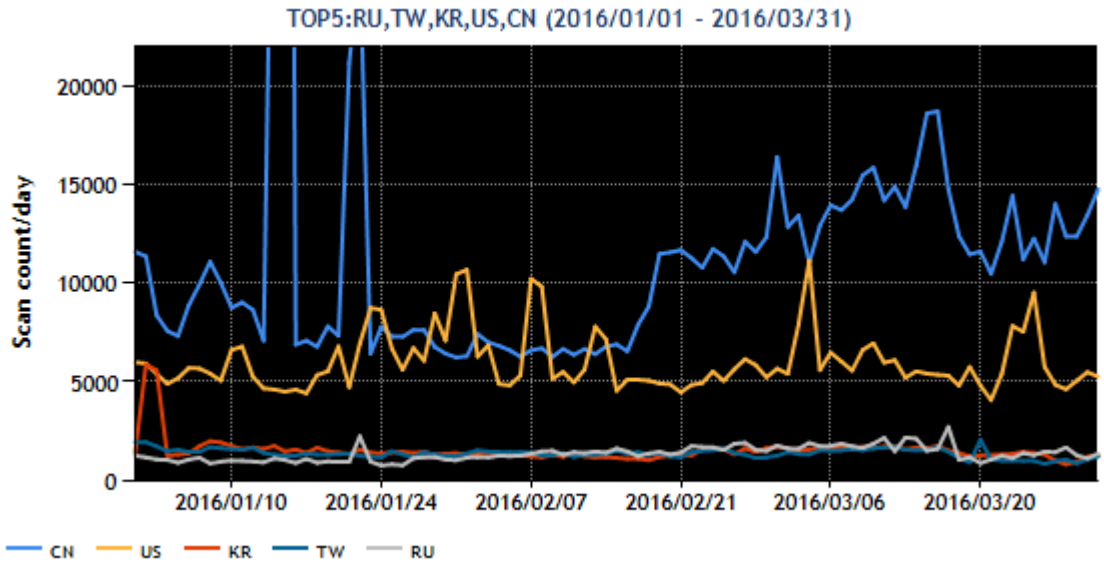
[図 1：2016 年 1~3 月の宛先ポート番号別パケット観測数トップ 5 の推移]

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	韓国	5
4	台湾	3
5	ロシア	4

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 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]

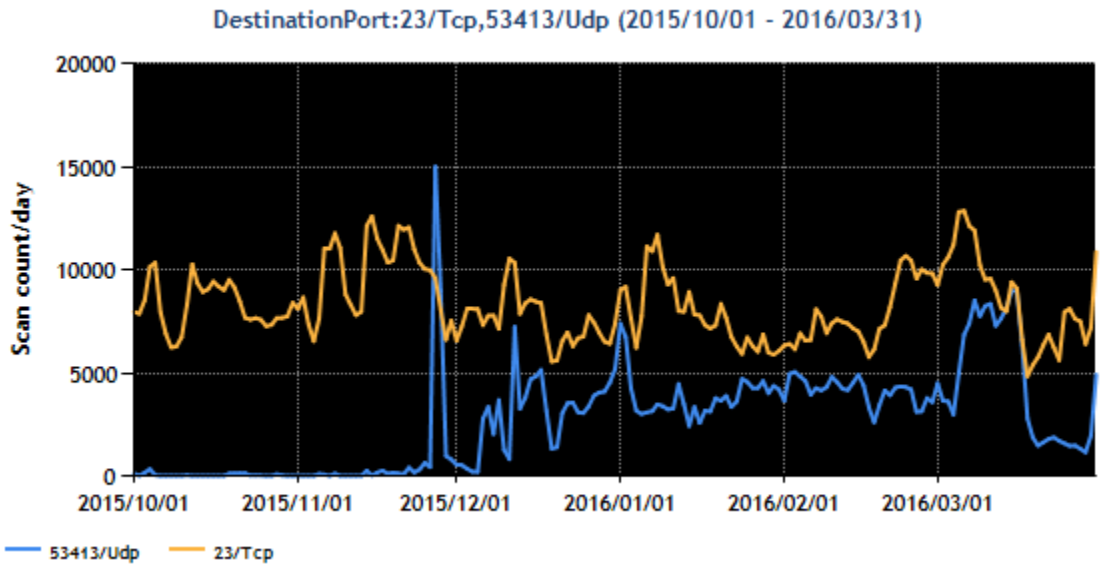
前四半期から本四半期にかけて、宛先ポート上位はそのままの順位で推移しました。また、ルータなど機器が使用するポートに対するパケット観測数が高い水準にあります。こうしたパケットの発信元はマルウエアに感染したと思われる機器が多くを占めています。日本国内からのパケット数は、全体の数の増減に埋もれてこのグラフからは傾向は、図 1 や図 2 ではわかりませんが、2016 年に入ってからは国内からの送信される事例が増加しています。こうした動向について「2.1 Port23/TCP 宛のパケット数の動向」で詳しく述べます。
その他については、多少の増減はありましたが、特筆すべき状況の変化は見られませんでした。

2　注目された現象

2.1　Port23/TCP 宛のパケット数の動向

2011 年 1 月ごろから様々な地域からの Port23/TCP 宛に対するパケットを観測しています。それらのパケット多くの送信元は、マルウエアに感染してボット化した設置されたルータや Web カメラなどの製品です。

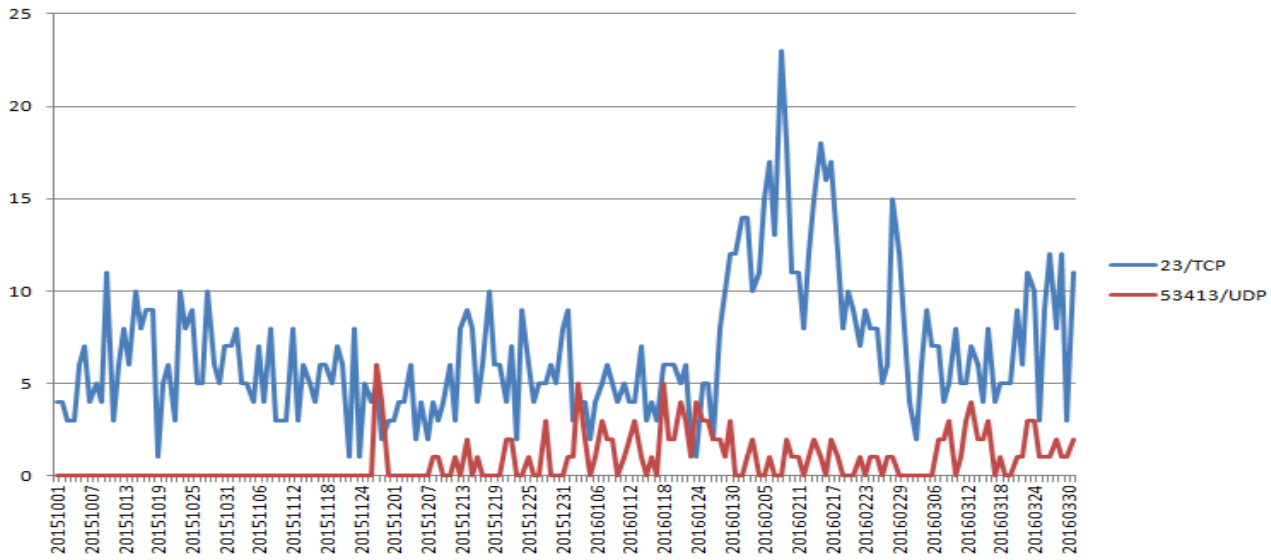
Port23/TCP 宛にパケットを送信するマルウエアは、JPCERT/CC では複数種存在していることを確認していますが、いずれも機器上で動作している Port23/TCP のサービス(Telnet)を対象とした探索後、機器に対して攻撃活動を行います。そうした感染機器の一部は、2015 年 11 月下旬以降、53413/UDP 宛のパケットも送信するようになりました。Port23/TCP と Port53413/UDP のそれぞれに宛てのパケット数の 2015 年 10 月以降の推移を図 3 に示します。



[図 3. Port23/TCP, PORT53413/UDP 宛のパケット数の推移]

JPCERT/CC では、不審なパケットの送信元 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、必要に応じて当該機器の製造ベンダ等や、関連 ISP 等に情報を提供し、問題点の解消に努めています。そうした事例を「JPCERT/CC インターネット定点観測レポート」[(*2)]でも、これまで数回にわたって紹介しております。

2016 年の 1 月中旬までは送信元の多くは海外からのパケットでしたが、1 月下旬に国内の送信元 IP アドレスからのパケットの増加がみられました。国内からの送信元 IP アドレス数の推移を図 4 に示します。



[図 4. 日本国内の IP アドレスから当該ポート宛にパケットを送信してきた IP アドレス数の推移]

調べてみると国内ベンダ製の次のような機器がマルウエアに感染した事例が複数みつかりました。

- 再生可能エネルギー設備のコントローラ機器
- 業務用通信機器
- 温度、湿度、気圧、水量などの情報を収集するための機器、等

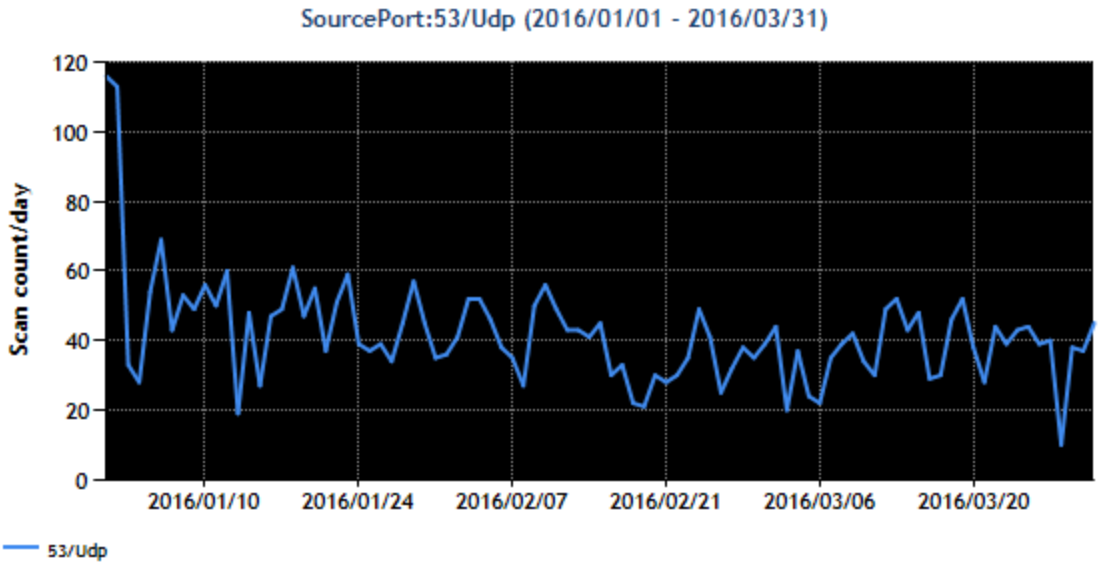
これらの機器は次のすべてもしくは一部に該当しました。

1. 量販店等で容易に購入できる製品でない
2. 内部ネットワーク等保護されたネットワーク環境での利用が推奨されている
3. Port23/TCP でサービス要求を待ち受けている
4. 安価な固定 IP アドレスサービスを提供している ISP に接続されている

不審なパケットを低減させるために、製品の開発者には製品の問題を、稼働中の機器が設置されている IP アドレスの管理者には稼働中の製品の問題を解消いただくよう JPCERT/CC から連絡しました。

2.2 国内のオープンリゾルバが送信元となっている DNS のリプライパケットの対応

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を含んだ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、オープンリゾルバに対して第三者が TSUBAME のセンサーの IP アドレスを詐称して送信し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 5 に示します。



[図 5. 53/UDP からのパケット観測数の推移]

オープンリゾルバは、DNS 水責め攻撃だけでなく、リフレクション攻撃にも悪用されるので、除去することが求められています。1 月下旬に複数の事業者が DDoS 攻撃を受けたとの報道[*3]がありましたが、その攻撃では複数のプロトコルが使用され、国内のオープンリゾルバを悪用したリフレクション攻撃も含まれていたと JPCERT/CC は推測しています。
JPCERT/CC では、該当パケットの送信元である 100 組織の管理者に情報を提供して善処を求めました。一部の管理者からは、対応結果について返信いただきましたが、その中には複数例のインターネットに接続された組込 Linux ボードがオープンリゾルバとなっていた事例や、機器ベンダが対策情報として公開しているフィルタルールの設定等をしないまま運用されていた事例が見つかりました。

JPCERT/CC では、稼働中の機器が設置されている IP アドレスの管理者に連絡を行ない、製品の問題と稼働中の製品の問題両方を解消できるよう努めております。

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) インターネット定点観測レポート
https://www.jpcert.or.jp/tsubame/report/index.html

(3) Threat Advisory: #OpKillingBay Expands Targets
https://community.akamai.com/docs/DOC-5781

本活動は、経済産業省より委託を受け、「平成２７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。