JPCERT/CC®

JPCERT-IA-2016-01
発行日：2016-02-04

JPCERT/CC インターネット定点観測レポート
[2015 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。

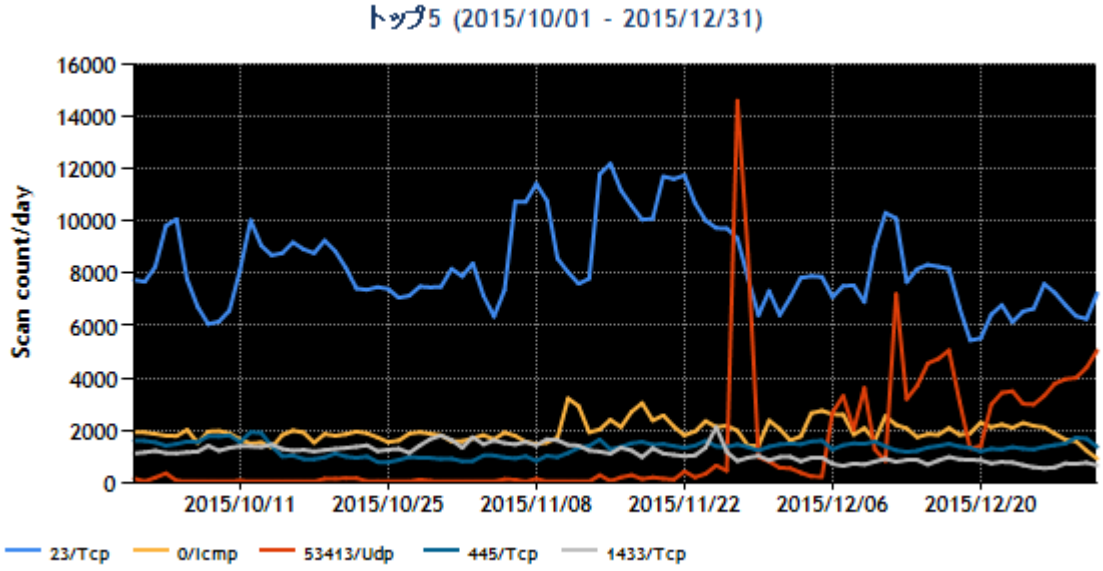
宛先ポート番号別パケット観測数のトップ 5 を [表 1]に示します。

[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	0/ICMP	2
3	53413/UDP	トップ 10 圏外
4	445/TCP (microsoft-ds)	3
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。



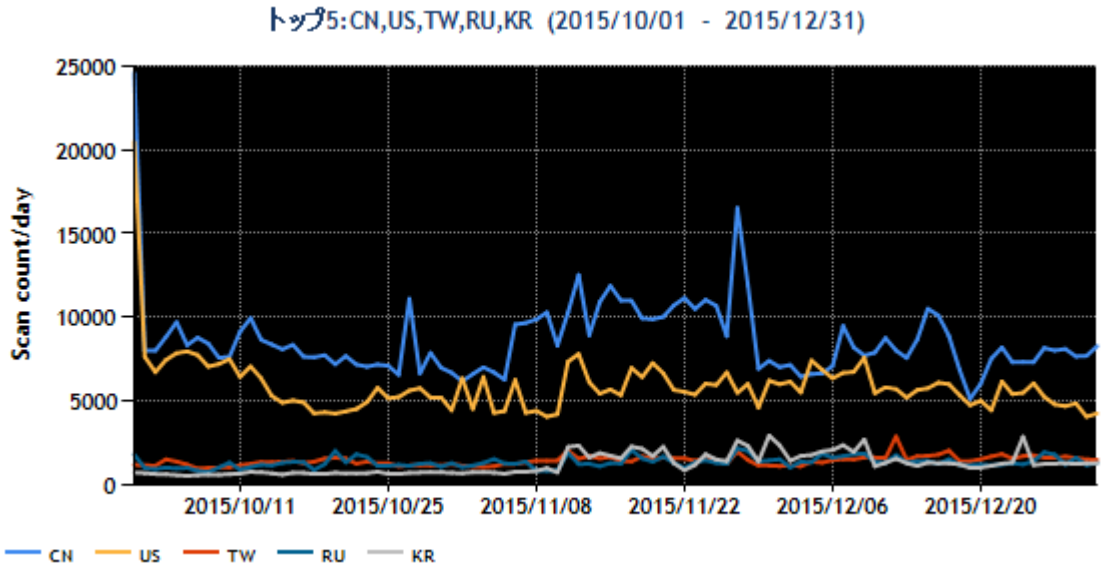
[図 1：2015 年 10~12 月の宛先ポート番号別パケット観測数トップ 5 の推移]

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	台湾	4
4	ロシア	7
5	韓国	8

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。



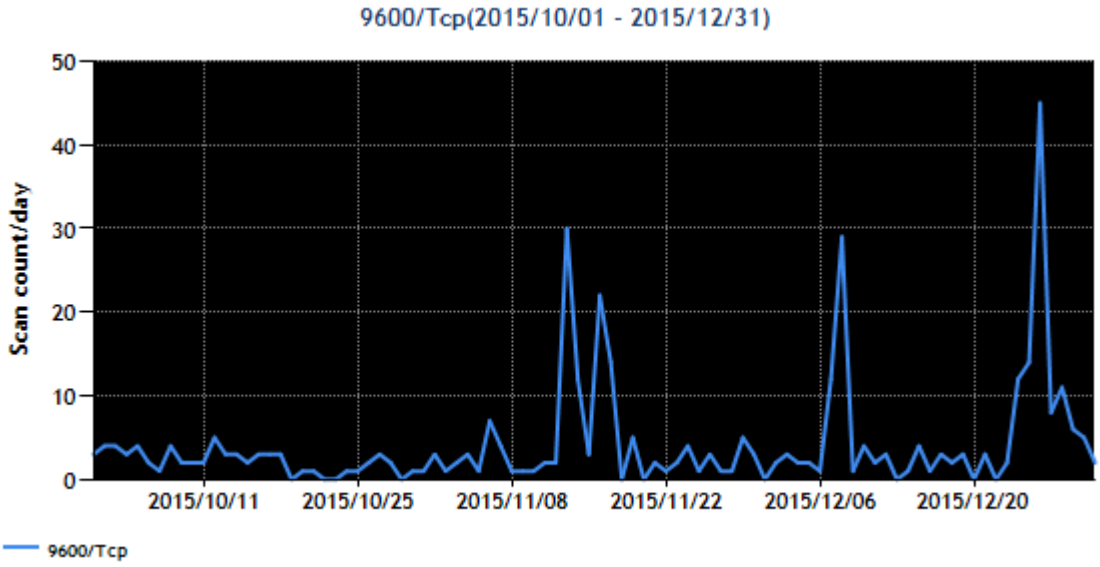
[図 2：2015 年 10~12 月の送信元地域別トップ 5 ごとのパケット観測数の推移]

本四半期は、前四半期に引き続き 23/TCP 宛のパケット数が高い水準にあります。一方、11 月 27 日～28 日には突発的に主に中国を送信元とする 53413/UDP 宛へのパケットが増加し、その後再び 12 月上旬から増加し続けて、期間中のパケット総数でも前四半期の圏外から第 2 位になりました。観測したパケットを分析した結果、53413/UDP を標準ポートとして使用する Netis/Netcore 社製のルータ製品を探索する目的のパケットと推測しています。この件については「2.2 IoT 機器を送信元としたルータ探索活動」でも関連事象を紹介しています。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　制御機器の探索を目的としたパケットとツールの存在

11 月中旬以降 9600/TCP 宛のパケット数の一時的な増加が数回発生しました。2015 年 10 月以降の観測数の推移を図 3 に示します。



[図 3. 9600/Tcp のパケットの観測数の推移]

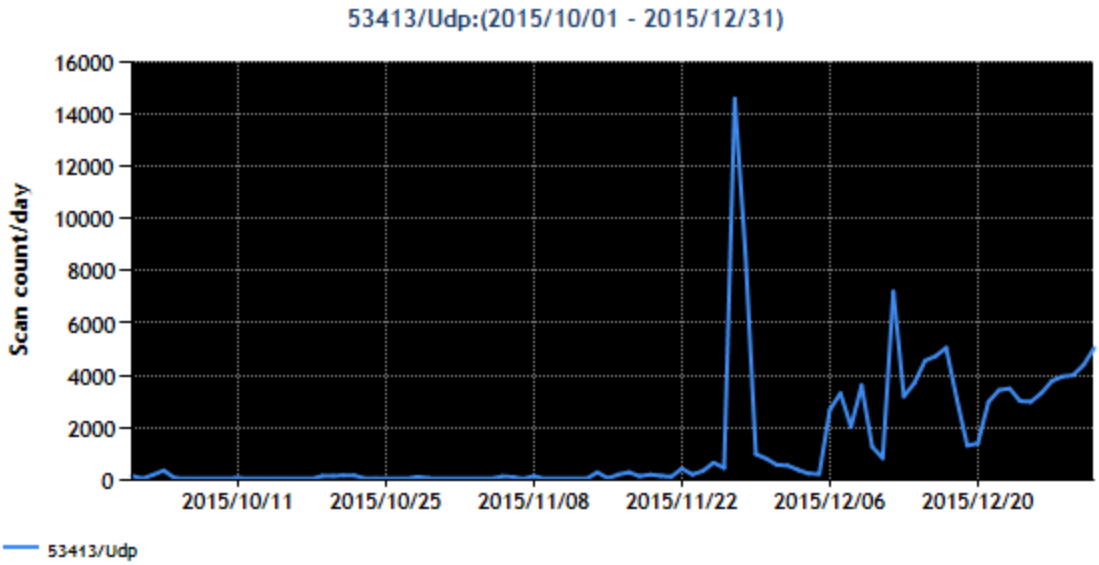
当該ポート番号は、一般的に使用されるソフトウェアのサービスで使用されるポート番号ではありません。そのため、このポート番号がどのようなサーバソフトウエアで使用されるのか、機器で使用されるのかを調査するところから分析作業を始めました。

また、最初に著しいパケット数の増加がみられた 11 月 13 日と 14 日には特定の IP アドレスから送信されたパケットが多くを占めました。そのため、この送信元 IP アドレスが過去どのようなポート番号に対する探索を行ったかを調査したところ、制御システムで使用されるポート番号に対する探索を行っていることが確認できました。制御機器などでこのポート番号が通信に使用されているかを調査したところ、国内制御機器ベンダのマニュアルなどから 9600/TCP で使用されていることがわかりました。さらに、パケットの送信元 IP アドレスに関する情報から、海外の制御システムで使用される機器のセキュリティ研究を目的としたとおもわれる団体が運営する Web サイトに行き当たりました。そして、パケット数が増加した時期に当該 Web サイトに掲載したと見られる、上述のベンダの製品に関するセキュリティ問題に関する記述と、その実証を目的としたとみられるコンセプトコードなどが公開されていました。

12 月 20 日頃からは、パケット数だけではなく送信元 IP アドレス数も増加しており、当該 Web サイトの閲覧者等からの探索も含まれているのではないかと推測されます。これらの状況から、制御システム用の機器も、セキュリティ研究の対象となっており、脆弱性やツールが公開されれば、興味本位の攻撃に晒されうると言えます。

2.2 IoT 機器を送信元としたルータ探索活動

第 1 章でも記載しましたが、11 月 27 日～28 日に主に中国を送信元とする 53413/UDP 宛へのパケット数が突発的に増加し、その後再び 12 月上旬から増加し続けています。2015 年 10 月以降の観測数の推移を図 4 に示します。



[図 4. 53413/UDP のパケットの観測数の推移]

このポート番号は、日本で広く利用されている製品では、ほとんど使用されていません。2014 年 8 月 27 日に公開されたトレンドマイクロ社のブログ記事によると、Netis/Netcore 社製のルータ製品に脆弱性があり、このポート番号に細工したパケットを送ることで、ルータが用意している任意のコマンドを遠隔の第三者がルータ上で実行できるとされています。この問題を修正するためのファームウエアの更新を 2014 年 9 月 5 日までに製品ベンダが行いました。この件は、インターネット定点観測レポート(2015 年 4～6 月)[(*2)]でも取りあげました。

修正ファームウエアの提供から 1 年以上経過しましたが、ファームウエアを更新せず、脆弱性を抱えたまま利用されている Netis/Netcore 社製のルータが多数インターネットに接続されているようです。[(*3)]

特に、そうした脆弱なルータを探索する目的と思われるパケットが 11 月中旬以降に増加しています。

探索パケットの中には、マルウエアに感染した Web カメラや、セットトップボックスなど、PC ではない機器から送信された事例を複数確認しており、一部は日本国内の機器と思われる IP アドレスも含まれていました。

PC ではない組込み機器がマルウエアに感染してボット化し、脆弱性が存在するルータを探索している、すなわち脆弱な組込み機器を使って他の脆弱な組込み機器を探索する活動が展開されているようです。

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) インターネット定点観測レポート(2015 年 4～6 月)
https://www.jpcert.or.jp/tsubame/report/report201504-06.html
(3) Vulnerable Netis Router Scanning Project
https://netisscan.shadowserver.org/

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。