JPCERT-IA-2017-01
発行日 ：2017-02-09

JPCERT/CC インターネット定点観測レポート
[2016 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。

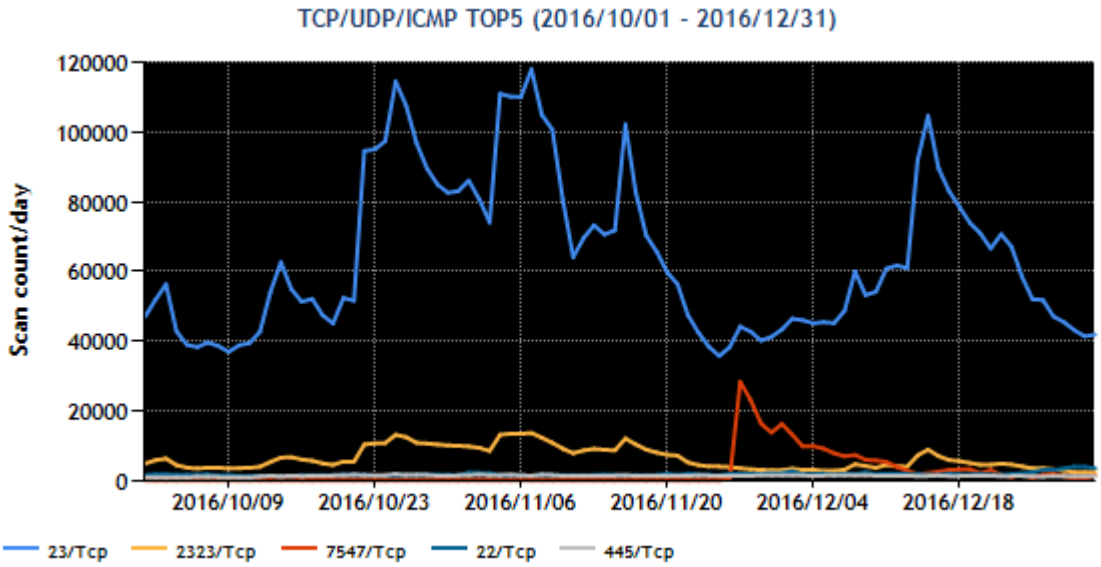
宛先ポート番号別パケット観測数のトップ 5 を［表 1］に示します。

［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	2323/Tcp	トップ 11 以下
3	7547/Tcp	トップ 11 以下
4	22/TCP	3
5	445/TCP (microsoft-ds)	4

※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。



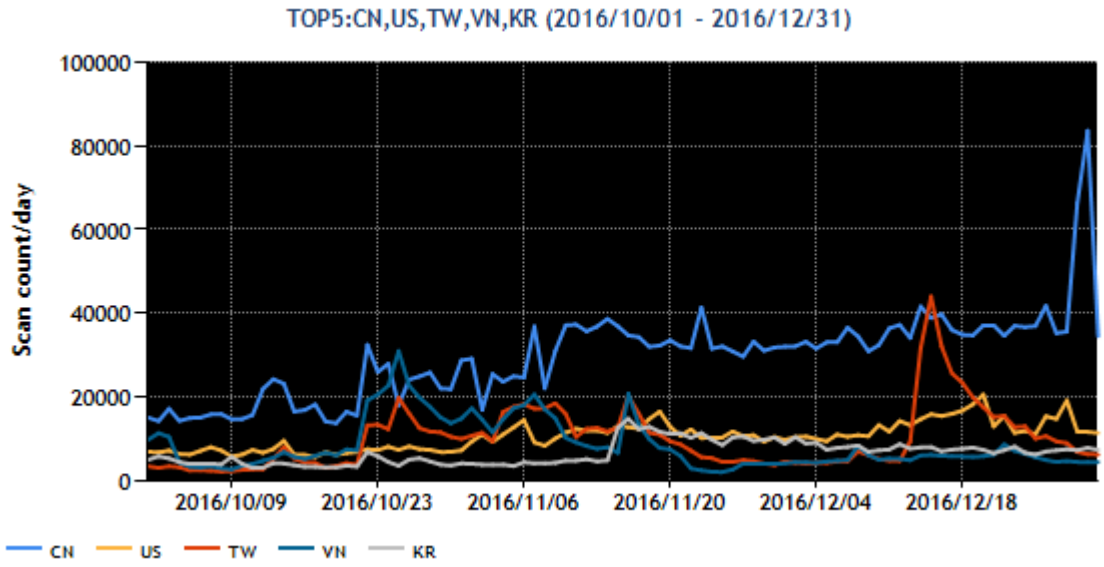
［図 1：2016 年 10～12 月の宛先ポート番号別パケット観測数トップ 5 の推移］

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	6
4	ベトナム	4
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。



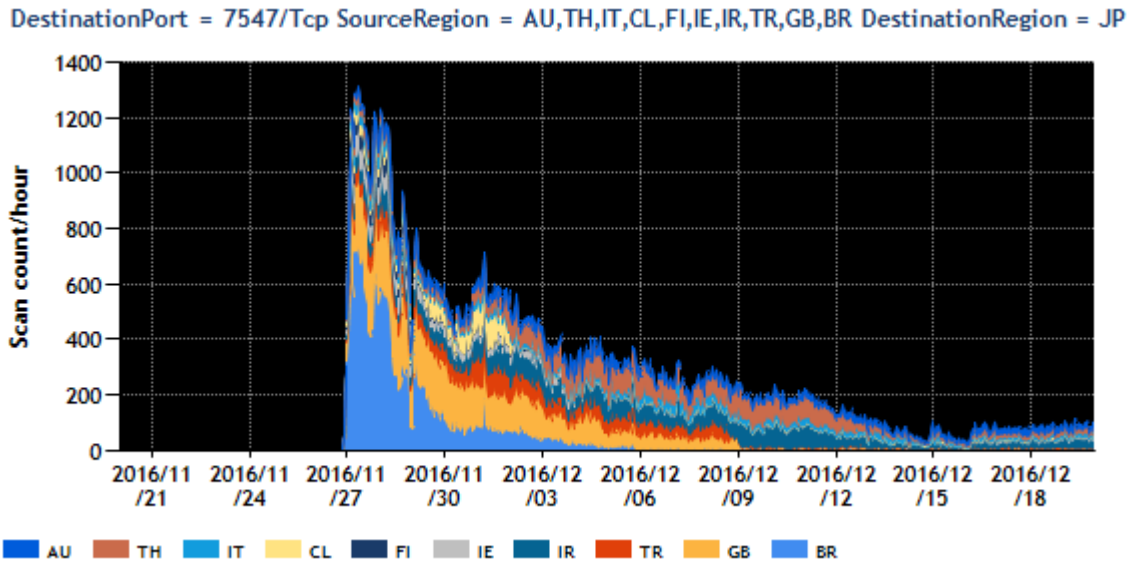
［図 2：2016 年 10～12 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

本四半期は、23/TCP を含めて、主に機器が使用していると思われるポートに対するパケットが増加し TOP3 を占めました。また、それ以外の複数のポートに対するパケットが増加しました。この増加については、「2.1 機器を対象としたパケット数の増加」で詳しく述べます。次に、送信元地域別のトップ 5 では、台湾が前四半期の 6 番目から 3 番目になりました。台湾が TOP5 に入った理由は、宛先ポート番号別の内訳で一番多く 55%近くを占めた 23/TCP 宛のパケットのおよそ 13%が台湾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　複数の機器宛のパケット数の増加

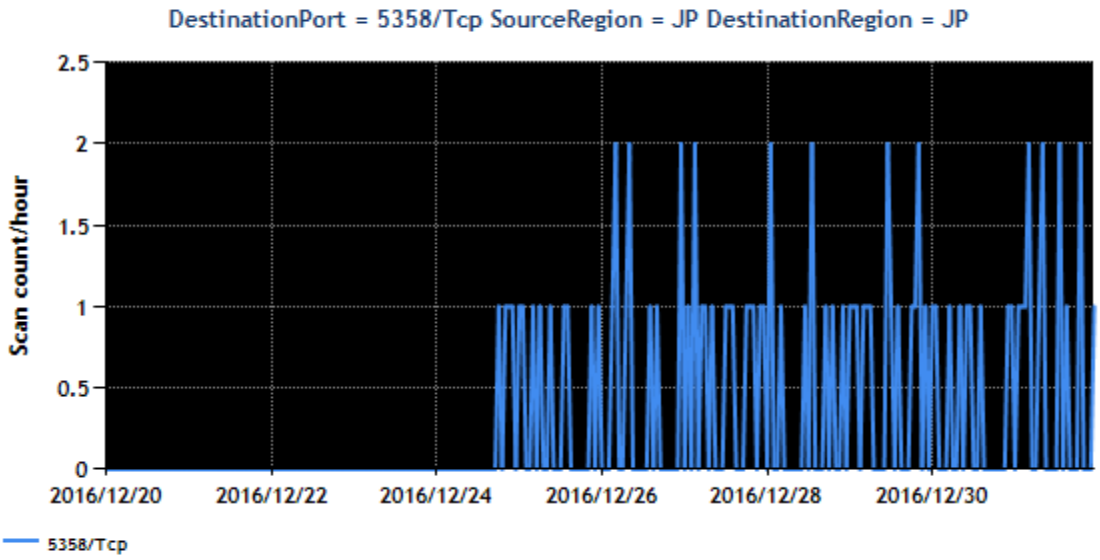
前回のインターネット定点観測レポート（2016 年 7～9 月）の「2.1Port23/TCP 宛のパケット数の増加」で、 Mirai と呼ばれるマルウエアの活動が盛んになっていることを記載しました。本四半期も Port23/TCP と Port2323/TCP 宛のパケットが増加した状態が続きました。また、前述の 2 つのいずれとも異なる複数のポートに対するパケットが観測され、Mirai のソースコードが公開されたことにより、Mirai の亜種が登場したことが推測されました。
図 1 で示したように、7547/TCP 宛のパケットが 3 番目に多く観測されました。地域別の変化を見るため、図 3 に上位 10 地域のグラフを示します。



［図 3：Port7547TCP 宛のパケットのトップ 10 ごとのパケット観測数の推移］

ブラジル・イギリス・トルコなど複数の地域からのパケットが、ほぼ同じタイミングで増加しましたが、その後次第に減っていきました。減少するスピードは地域により差異がありました。パケットの送信は多くの地域で ISP への接続に使用するネットワーク機器の脆弱性(*2,3,4)によるものと報じられました。それらの情報をもとに製品情報を調査したところ、複数の製品が該当しました。しかし、ユーザに機器を配布する際は、メーカの型番ではなく ISP にて新たに型番を付ける場合が多く、型番から製品を特定することが難しいため、パケットが多く送信された地域の ISP では、修正ファームウエアの提供を ISP が呼びかけたり、停止したルータの復旧方法をアナウンスしたりするなどの対応に追われたようです。こうしたことから、JPCERT/CC では、海外の型番をもとにして、国内で使用されている脆弱な機器を検索することは困難であると考え、マルウエアに感染した機器が踏み台となる事象が発生しているかどうかをみるために、国内の障害情報等について情報を収集しました。当該期間のパケットは 1 パケットのみであったことに加え、障害や緊急対応を行ったなどのアナウンスや報道も確認されていないため、日本国内への影響は小さかったのではないかと推測されます。

続いて、2016 年 12 月 24 日ごろから観測された、国内の IP アドレスを送信元とする Port5358/TCP に対するパケットの推移を図 4 に示します。

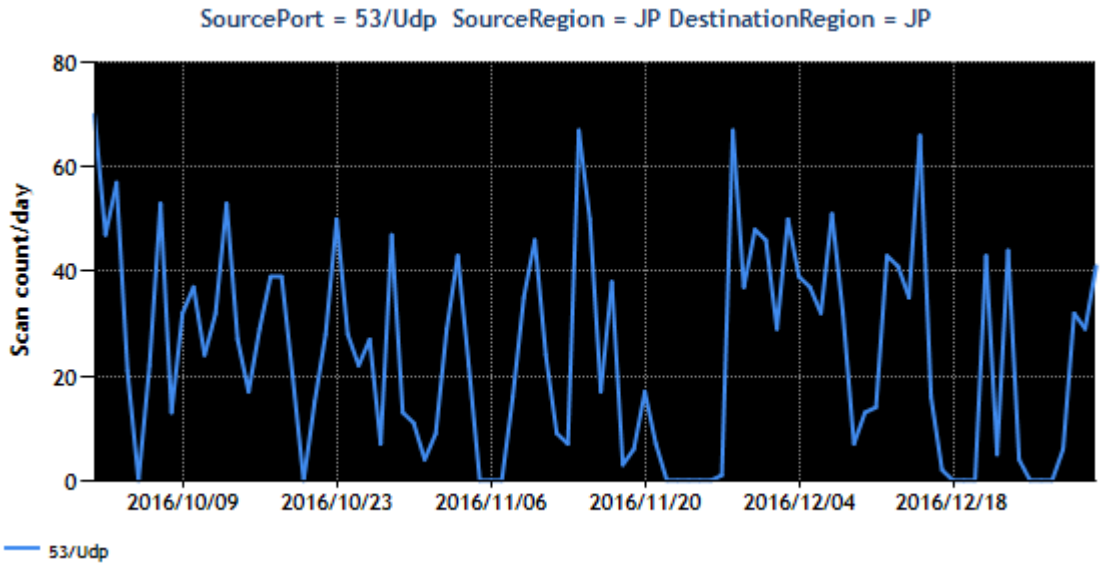


［図 4：Port5358/TCP 宛のパケット観測数の推移］

12 月 24 日以前のパケットの送信状況を確認したところ、これらの送信元 IP アドレスから Mirai の特徴をもつパケットを Port23/TCP や Port2323/TCP に対して送信していました。このことから、パケットの送信元に設置されていた機器は既に Mirai に感染していたと推測できます。
不審なパケットを低減させるために、JPCERT/CC ではこれまでもパケットの送信元に設置されている機種の推定を行ってきました。今回も JPCERT/CC では Mirai、もしくは亜種のマルウエア挙動が変わった可能性があると考え、これらのホスト群を調査しました。その結果、送信元には共通する特徴があることがわかり、機種の特定には到りませんでしたが、機器に関するいくつかのヒントを得ることができました。TSUBAME での観測データと推定された機器の情報を関係すると思われる機器ベンダに提供しました。また、5358/TCP へパケットを送信する IP アドレスの管理者（多くは ISP）にパケットログの情報を提供しました。
その結果、ISP から情報を受けとったユーザが製品ベンダに連絡をしたとみられ、発生している現象に関する調査が行われ、機器がマルウエアに感染する経緯が特定されました。
当該製品は、ある条件を満たした場合にのみマルウエアに感染します。JPCERT/CC では、継続してマルウエアの挙動に関する情報をベンダに提供し、対策の検討に役立てていただいています。また送信元 IP アドレスの管理者に対する連絡を強化しています。
その後も、既知の脆弱性が存在する監視カメラ製品のポートに対して、Mirai に感染していると思われる機器がパケットを送信するなどの事象(*5,6)が見られました。攻撃者は Mirai およびその亜種を使って、インターネットからアクセス可能な機器に対して探索活動を行い、脆弱性への対応が行われていない、初期パスワード等をそのまま使用しているといったセキュリティ上問題がある機器に対して攻撃をおこなっていると推測されます。

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 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改善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) New Variant of Mirai Embeds Itself in TalkTalk Home Routers
https://www.incapsula.com/blog/new-variant-mirai-embeds-talktalk-home-routers.html

(3) New Mirai Worm Knocks 900K Germans Offline ?
https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/

(4) TR-069 NewNTPServer Exploits: What we know so far
https://isc.sans.edu/forums/diary/TR069+NewNTPServer+Exploits+What+we+know+so+far/21763/

(5) 「Mirai」ボットの亜種等からの感染活動と見られるアクセスの急増について
https://www.npa.go.jp/cyberpolice/detect/pdf/20170120.pdf

(6) インターネットに接続された機器の管理に関する注意喚起
https://www.jpcert.or.jp/at/2016/at160050.html

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。