Japan Computer Emergency Response Team Coordination Center

電子署名者 : Japan Computer Emergency Response Team Coordination Center
DN : c=JP, st=Tokyo, l=Chiyoda-ku, email=office@jpcert.or.jp, o=Japan Computer Emergency Response Team Coordination Center, cn=Japan Computer Emergency Response Team Coordination Center
日付 : 2018.01.17 18:32:24 +09'00'

JPCERT-TBM-2018-01
発行日 : 2018-1-18

JPCERT/CC インターネット定点観測レポート
[2017 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。また、こうした観測では、複数の視点による多元的な見方も重要であるため、主に海外の National CSIRT と連携してそれぞれの組織にセンサーを設置し観測網に参加してもらう活動を行っています。各地のセンサーから収集したデータを分析し、問題が見つかれば、適切な地域の National CSIRT 等に情報を提供し、状況の改善を依頼しています。また、日本国内固有の問題については、JPCERT/CC の日々の活動の中で対処しています。
本レポートでは、本四半期に国内に設置されたセンサーで観測されたパケットを中心に分析した結果について述べます。

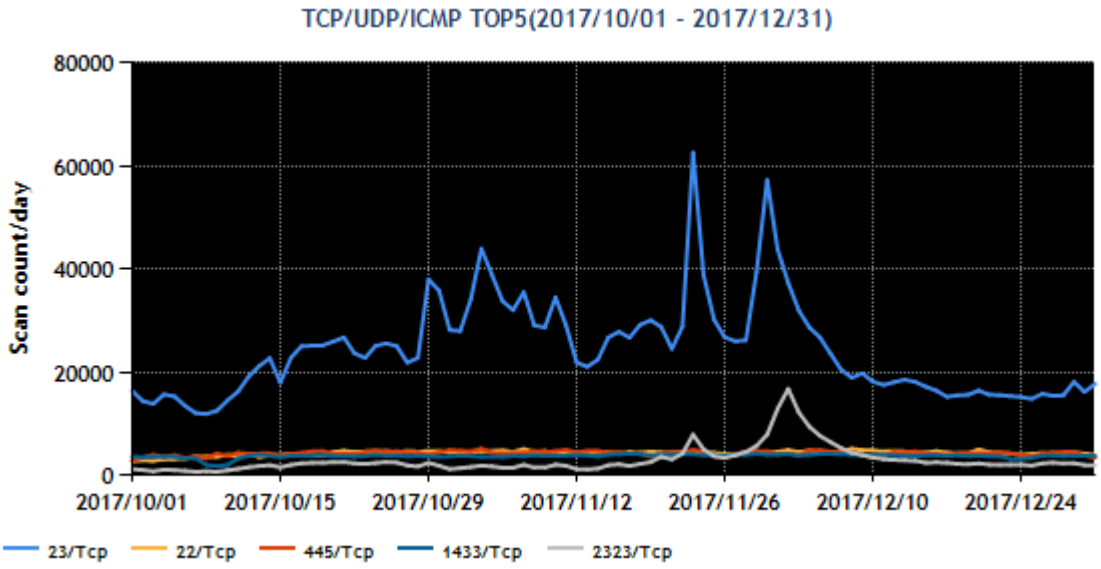
宛先ポート番号別パケット観測数のトップ 5 を［表 1］に示します。

［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	22/TCP (ssh)	3
3	445/TCP(microsoft-ds)	4
4	1433/TCP(ms-sql-s)	2
5	2323/TCP	6

※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。



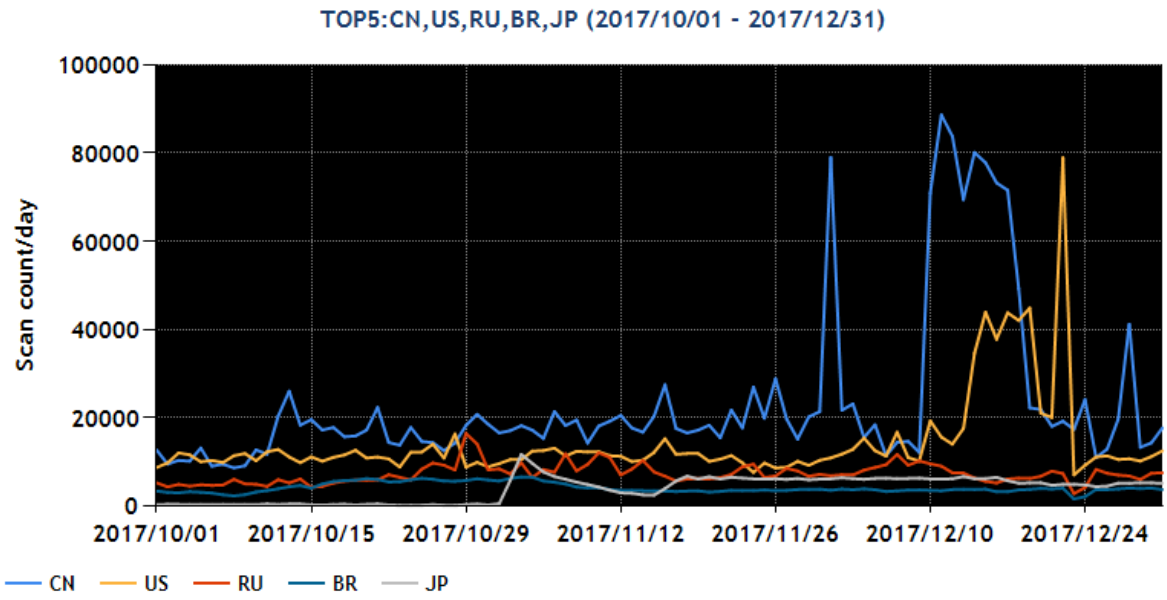
［図 1：2017 年 10～12 月の宛先ポート番号別パケット観測数トップ 5 の推移］

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	ロシア	3
4	ブラジル	7
5	日本	TOP10 外

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。



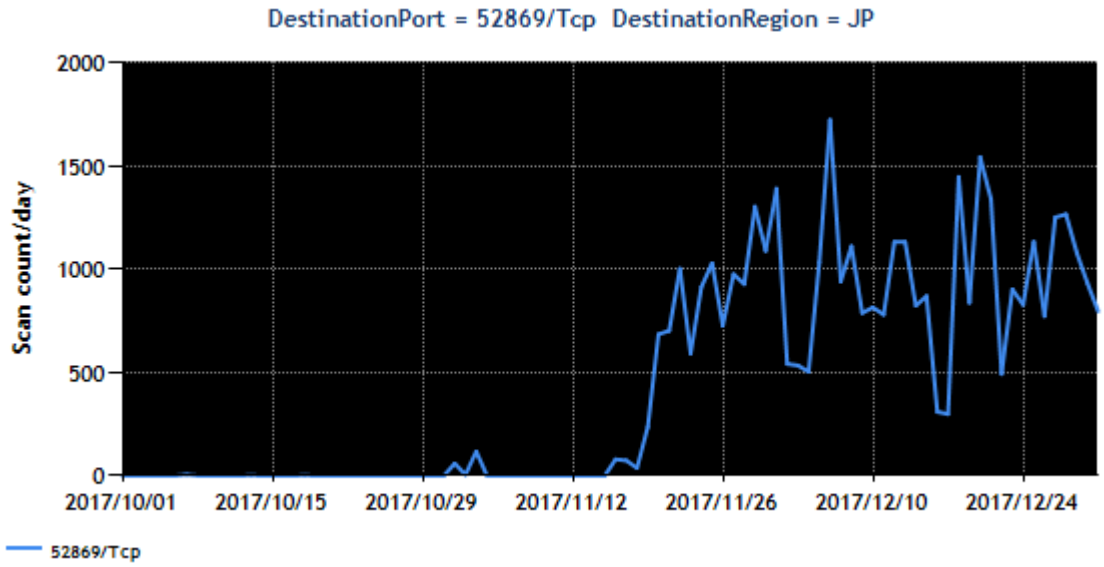
［図 2：2017 年 10～12 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

本四半期は、前四半期同様 Windows の SQLServer と SMB サービスのリクエスト受付用ポート向けのパケットが多数観測されました。また、前四半期もトップ 5 に入っていた、SSH（22/TCP）や Telnet（23/TCP）のリクエスト受付用ポート向けのパケットも継続して観測しており、脆弱な Web カメラ、ルータ、NAS 等の機器の探索が継続して行われているものと推測されます。また、送信元地域別の 5 番目に日本が入り、その理由として、日本国内で多くの使用者がいると思われる無線 LAN 機器が脆弱性を悪用した攻撃を受け、Mirai 亜種に感染したことが考えられます。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. 52869/TCP 宛のパケットの観測状況について

10 月 30 日頃、及び 11 月 15 日頃から、52869/TCP 宛のパケットを観測しています（図 3）。

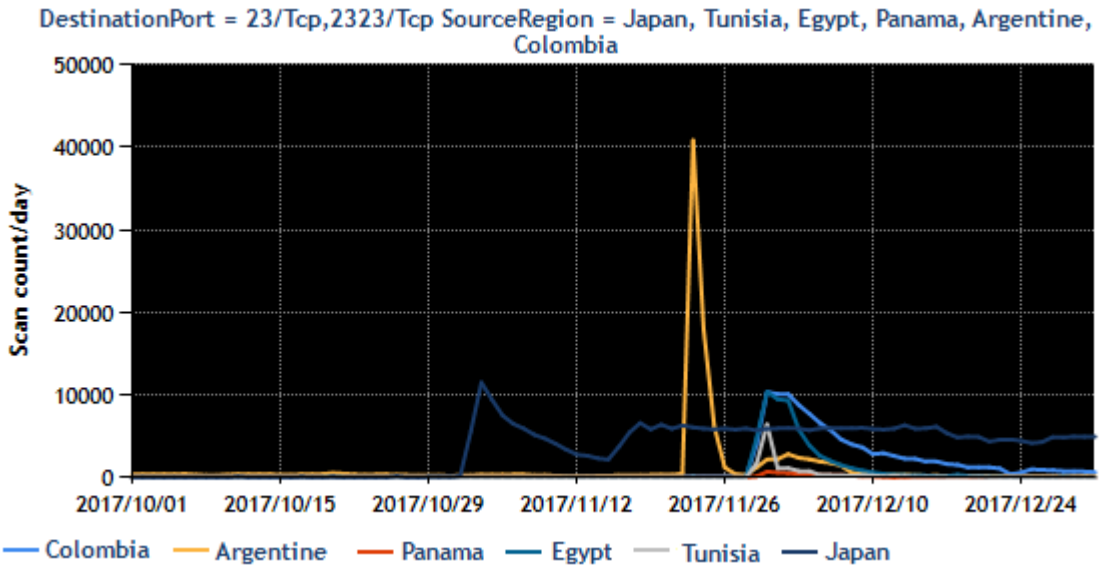


［図 3：Port52869/TCP 宛のパケットの観測数の推移］

TSUBAME のセンサーは日本を含む 21 経済地域に設置していますが、この種のパケットを観測したセンサーのほぼすべてが日本国内に設置されたものでした。本傾向は 11 月までみられ、12 月以降は海外のセンサーでも観測しています。このポートをスキャンするパケットの目的は 2015 年の 4 月に公開(*2)された Realtek SDK Miniigd サービスの脆弱性をもつホストの探索だと推測されます。本脆弱性はすでに攻撃コードがインターネット上に公開されているため、容易に攻撃を行うことが可能です。また、JPCERT/CC では、日本国内で普及しているルータの一部で古いファームウエアを使用している場合に本脆弱性の影響を受けることを確認(*3)したことから、早期の対策を呼びかけるために、2017 年 12 月 19 日に注意喚起を発行(*4)しました。また、他の組織からも本件に関する注意(*5)が呼びかけられています。

2.2. 23/TCP,2323/TCP 宛のパケット数の観測状況について

図 4 は 23/TCP または 2323/TCP 宛の観測パケット数の推移を、主な送信元地域ごとに示したものです。10 月末頃から、それ以前にはなかった数のパケットが観測されるようになりました。



［図 4. Port23/TCP または Port2323/TCP 宛の観測パケット数の主な送信元地域ごとの内訳の推移］

これらのパケットは、Mirai に感染した端末からのパケットと共通した特徴を有しており、Mirai の亜種に感染した端末によるものと推測されます。また、日本国内から送信された 23/TCP 宛のパケットの送信元となっている感染した端末の機種を特定するため、一部の送信元にアクセスして確認してみましたが、52869/TCP が開いていること以外には機種を特定できる情報は得られませんでした。

23/TCP のパケットは図 4 に示したように 10 月 30 日頃から観測され始めましたが、これは 2.1 で述べた 52869/TCP のパケットを一時的に観測した時期とほぼ一致しています。23/TCP のパケットはその後 11 月 14 日にかけて減少しましたが、これも 2.1 で述べた 52869/TCP のパケットを観測しなかった時期と一致しています。また 11 月 15 日以降は、52869/TCP のパケットが再び観測されるとともに、日本国内からの 23/TCP のパケットも増加に転じ、その後はほぼ一定のパケット数が続いています。こうした観測パケット数の推移から、52869/TCP のパケットによって脆弱な端末が探索されて、Mirai の亜種に感染し、23/TCP 宛のパケットを送信するようになったシナリオを一つの可能性として描くことができます。

なお、11 月 15 日からは、23/TCP 宛ばかりでなく 2323/TCP 宛のパケットも観測されるようになりました。

送信元の地域も、日本ばかりでなく、11 月 23 日頃にはアルゼンチン、11 月 29 日頃にはコロンビア、パナマ、エジプト、チュニジアなどに拡大(*6)しています。いずれの地域のケースも脆弱性をもつインターネット接続機器(*7)が攻撃を受け Mirai の亜種に感染したと推測されます。

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

(2) (0Day) Realtek SDK miniigd AddPortMapping SOAP Action Command Injection Remote Code Execution
http://www.zerodayinitiative.com/advisories/ZDI-15-155/

(3) ロジテック製 300Mbps 無線 LAN ブロードバンドルータおよびセットモデル (全 11 モデル)に関する重要なお知らせとお願い
http://www.logitec.co.jp/info/2017/1219.html

(4) Mirai 亜種の感染活動に関する注意喚起
https://www.jpcert.or.jp/at/2017/at170049.html

(5) ルータ製品の脆弱性を悪用して感染を広げる Mirai の亜種に関する活動(2017-12-19)
http://www.nicter.jp/report/2017-01_mirai_52869_37215.pdf
脆弱性が存在するルータを標的とした宛先ポート 52869/TCP に対するアクセス及び日本国内からの Telnet による探索を実施するアクセスの観測等について
https://www.npa.go.jp/cyberpolice/important/2017/201712191.html
Mirai 亜種の感染拡大に伴う注意喚起
https://wizsafe.iij.ad.jp/2017/12/175/

(6) 国内における Mirai 亜種の感染急増 (2017 年 11 月の観測状況)
https://sect.iij.ad.jp/d/2017/12/074702.html

(7) Security Notice - Statement on Remote Code Execution Vulnerability in Huawei HG532 Product
http://www.huawei.com/en/psirt/security-notices/huawei-sn-20171130-01-hg532-en

本活動は、経済産業省より委託を受け、「平成 29 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。