JPCERT Coordination Center

JPCERT/CC インターネット定点観測レポート

2020 年 4 月 1 日 ～ 2020 年 6 月 30 日

一般社団法人 JPCERT コーディネーションセンター

2020 年 7 月 30 日

JPCERT CC®

目次

1. 概況

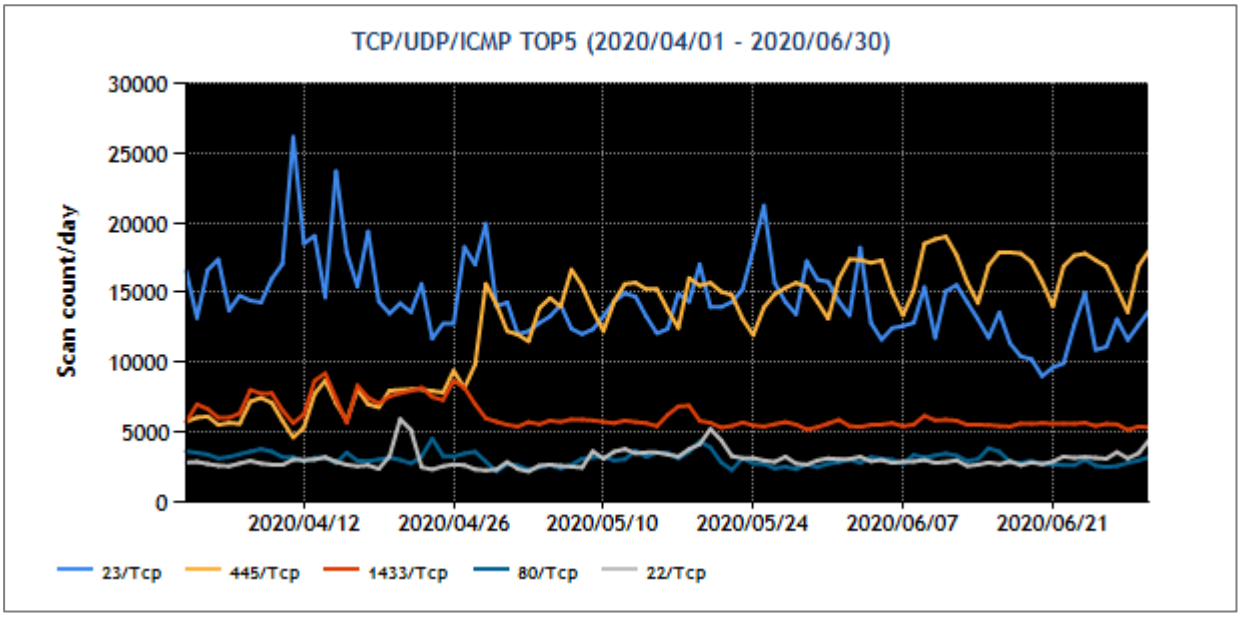
JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、不特定多数に向けて発信されるパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類して、これを脆弱性情報、マルウェアや攻撃ツールの情報などと対比して分析することで、攻撃活動や準備活動の捕捉に努めています。また、こうした観測では、複数の視点による多元的な見方も重要であるため、主に海外の National CSIRT と連携してそれぞれの組織にセンサーを設置し観測網に参加してもらう活動を行っています。
各地のセンサーから収集したデータを分析し、問題が見つかれば、適切な地域の National CSIRT 等に情報を提供し、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)	3
3	1433/TCP (ms-sql)	2
4	80/TCP(http)	4
5	22/TCP	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。



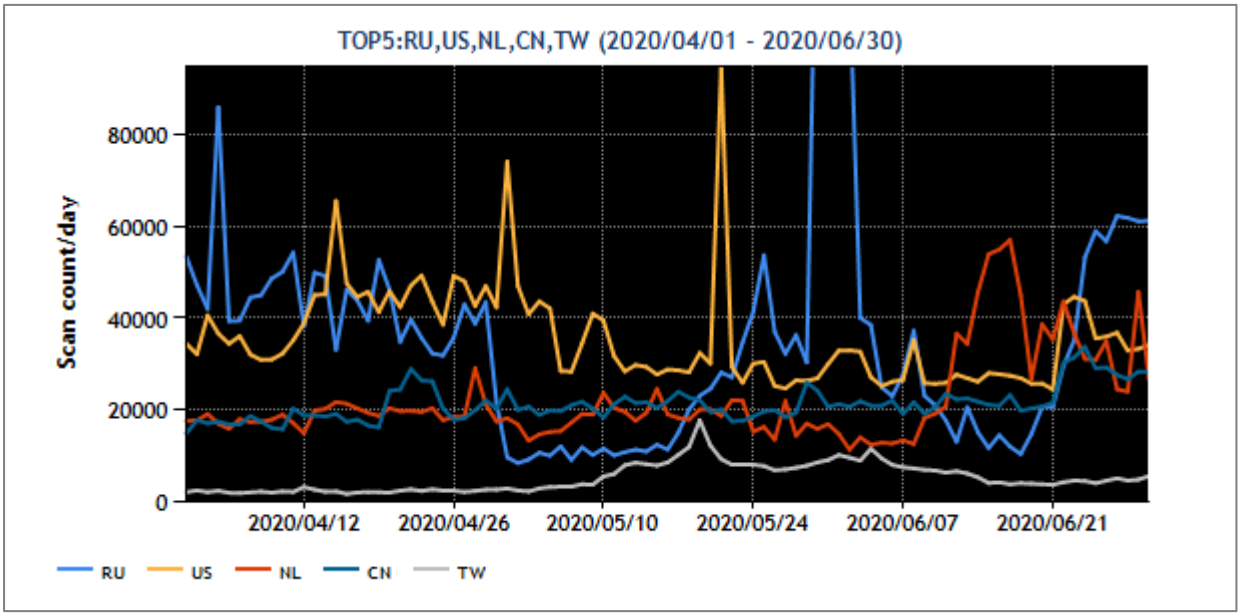
［図 1：2020 年 4～6 月の宛先ポート番号別パケット観測数トップ 5 の推移］

最も多く観測されたパケットは、本四半期も継続して 23/TCP （telnet）宛の通信でした。2 番目に多かった 445/TCP 宛の通信が 4 月下旬から増加しました。同じ時期に 1433/TCP は減少しており、両ポートがともに Windows 環境で使用されるものなので、両者の変化について関連性を調査しています。
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	ロシア	1
2	米国	3
3	オランダ	2
4	中国	4
5	台湾	9

［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。



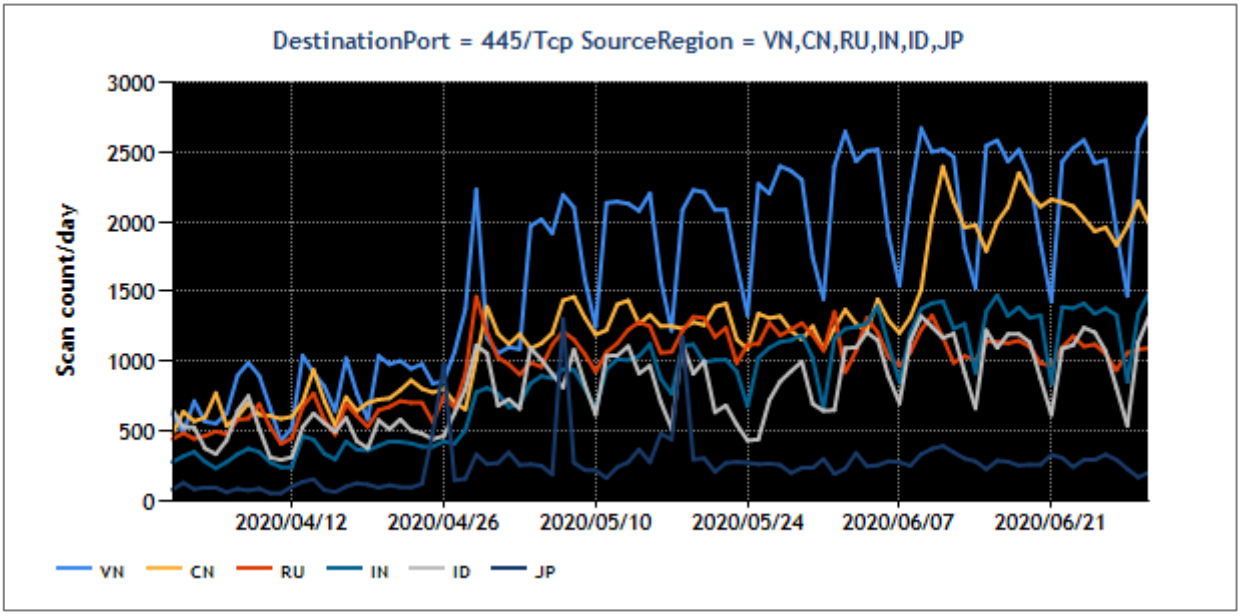
［図 2：2020 年 4～6 月の送信元地域別トップ 5 ごとのパケット観測数の推移］

本四半期に受信したパケットの送信元地域として、最も多く見られたのはロシアでした。ロシアを送信元地域としたパケットの TOP5 の宛先ポート番号は他の地域と大きな違いはありません。しかし、宛先ポート番号を TOP5 に限ったパケット数は、2 位以下の地域と比べてむしろ少なくなっています。それでも総数で上回った理由は、TOP5 以外のポート宛のパケットの多さにあります。特定のポートではなく、広範囲のポートについて開放状況を調査することを目的としたパケットの送信(2)と考えられます。2 位のオランダについてもロシアと同様の傾向でした。その他の地域については、順位に変化はありません。

2. 注目された現象

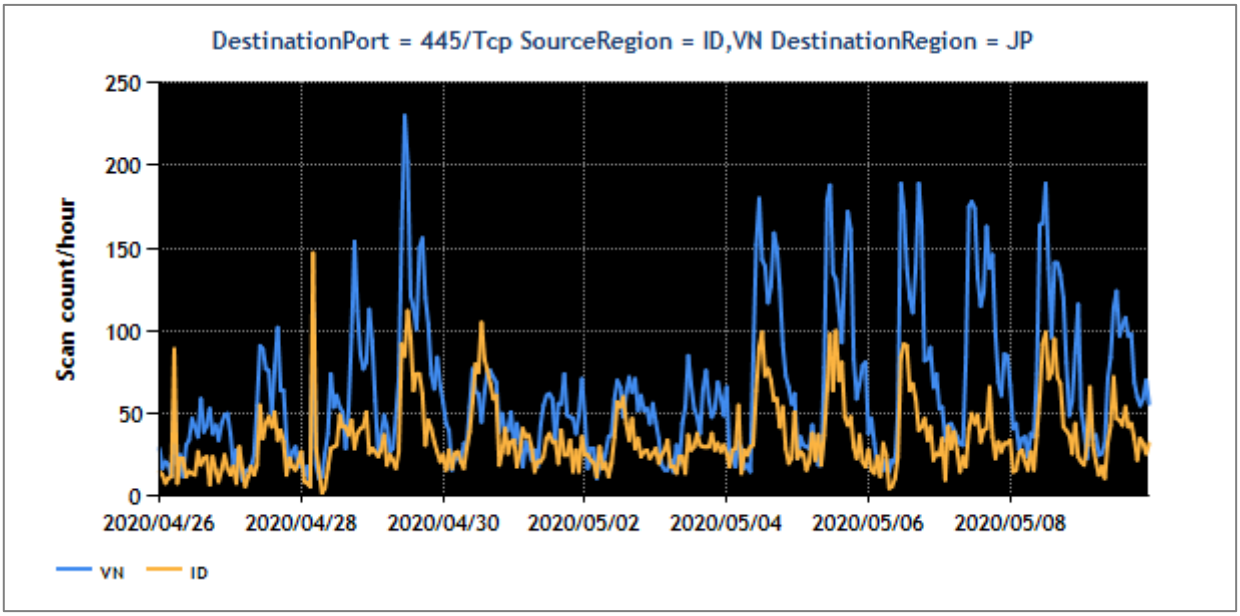
2.1. Port445/TCP 宛のパケット数の増加

2020 年 4 月 28 日頃から、複数の地域から送信された 445/TCP 宛のパケットが増加しています。送信元地域別トップ 5 に日本を加えたパケット観測数の推移を［図 3］に示します。

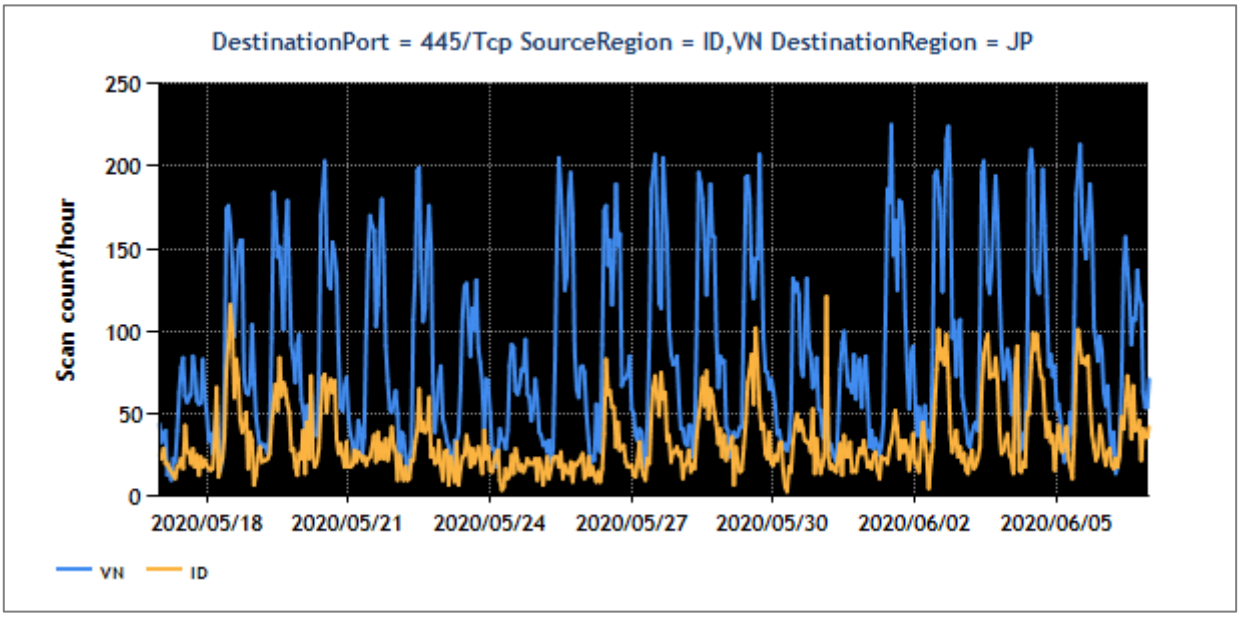


［図 3 : 2020 年 4～6 月の宛先ポート番号別パケット観測数トップ 5 の推移］

ベトナムから送信されたパケットを一番多く観測しています。また、パケット観測数は、1 週間の周期で変化しているようにも見えます。観測したデータを見てみると、ベトナムとインドネシアにそうした傾向が特にみられます［図 4、図 5］。



［図 4：4 月 26 日～5 月 9 日にかけてのベトナムとインドネシアを送信元とするパケット数の推移］



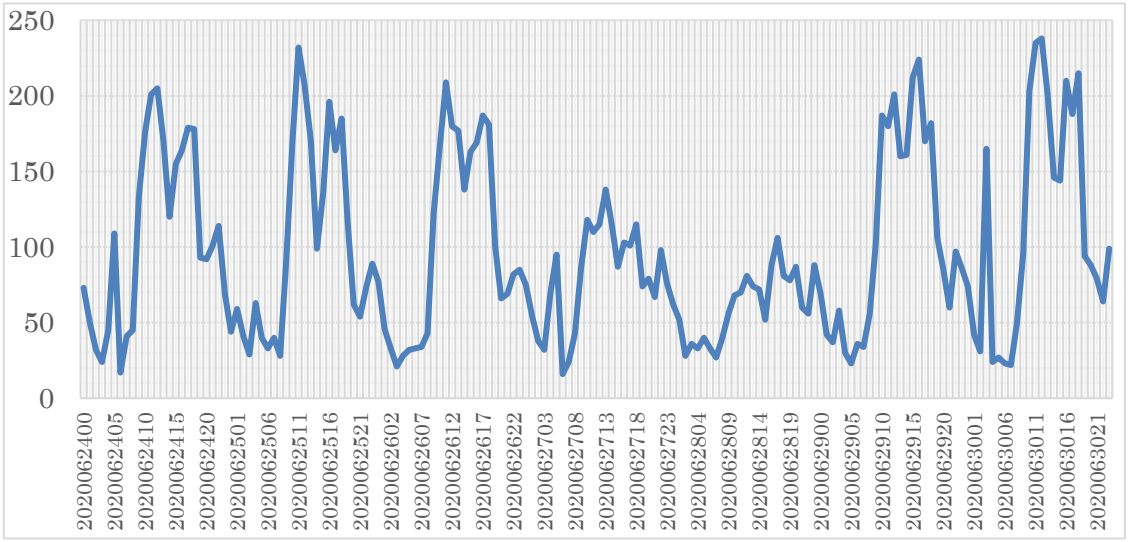
［図 5：5 月 17 日～6 月 6 日にかけてのベトナムとインドネシアを送信元とするパケット数の推移］

［図 4、図 5］から、ベトナムとインドネシアからのパケット観測数が落ち込む日時を見直してみると、土曜日や日曜日、祝日［表 3］といった時間帯にパケットの観測数が減少しているように見えます。

［表 3：ベトナムとインドネシアの祝日のリスト］

観測日	地域	祝日名
4 月 30 日	ベトナム	南部ベトナム解放記念日
5 月　1 日	ベトナム、インドネシア	メーデー
5 月　7 日	インドネシア	ワイサック
5 月 21 日	インドネシア	キリスト昇天祭
5 月 22 日	インドネシア	政令指定休日
5 月 24 日	インドネシア	ラマダン
5 月 25 日	インドネシア	ラマダン
6 月　1 日	インドネシア	パンチャシラの日

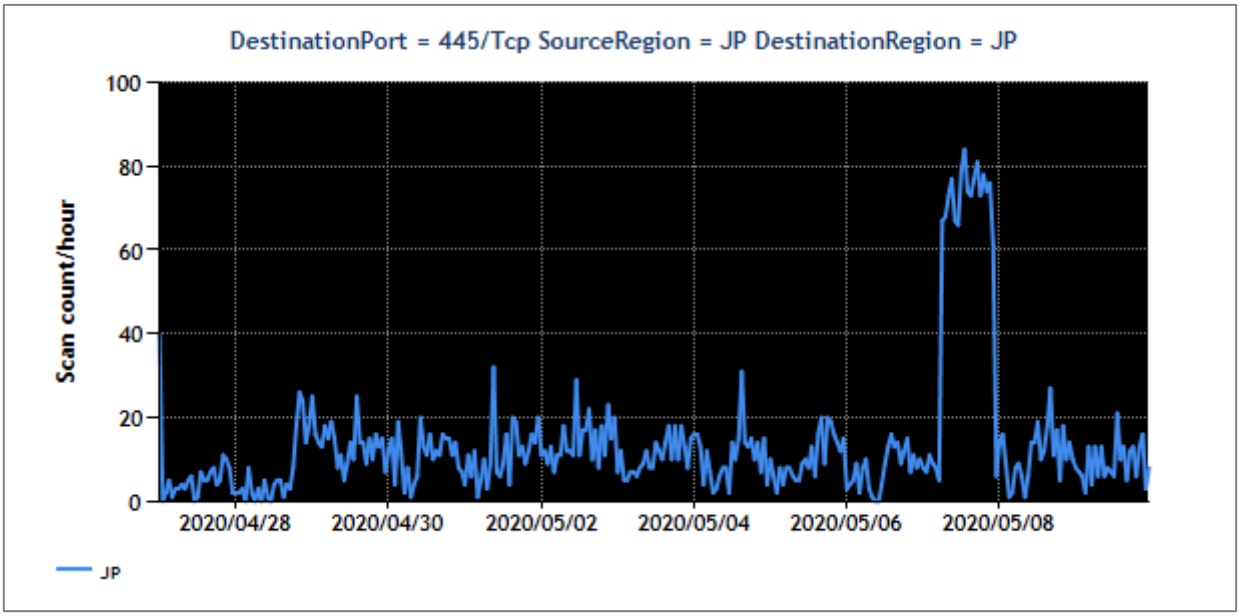
もう少し細かく時間帯別の傾向を見るため、6 月 24 日から 30 日までのベトナムから送信されたパケットを 1 時間単位で集計したものを［図 6］に示します。



［図 6：2020 年 6 月 24 日～6 月 30 日にかけてベトナムを送信元としたパケット数の推移］

［図 6］の横軸は日本時間での表示(GMT+9)であり、-2 時間したものが現地時間となります。おおよそ現地時間の 7～8 時ぐらいから増え始め、12 時に一時的に少なくなり、13 時に再度増え、19 時には少なくなるという規則性が読み取れます。これはベトナムのビジネスアワーとほぼ一致します。このパケットを発生させている原因は定かではありませんが、仮にマルウェアが関係していたと考えると、マルウェアに感染した PC の起動と停止に応じてパケット観測数が変化していると推測できます。平日に PC を使用する職場や学校などの PC がマルウェアに感染している恐れがあると考え、観測されたデータを当該地域の National CSIRT に提供しました。

最後に日本を送信元としたパケットの状況を見ておきます。日本は TOP5 ほどのパケット量ではありませんが、4 月 28 日頃から 445/TCP 宛のパケットの増加を観測しています。［図 7］



［図 7：4 月 27 日～5 月 9 日にかけての日本からのパケットの推移］

しかし、［図 7］は［図 5］と異なり特定の曜日や祝日にパケット数が減少するような傾向は、確認できません。また、［図 6］とも異なり 1 日の間でのパケットを観測する時間帯も広くなっていて、深夜以外にパケット数が減少する時間帯はないといった傾向の違いがみられます。
JPCERT/CC では、これらのパケットのうち、日本国内から発信され発信元が企業等とみられるものについて、当該 IP アドレスの管理者全てに連絡を行って本件に関する情報を収集しています。
連絡があった際は、可能な範囲での調査を行い、差し支えなければ結果をお知らせください。当該現象の理解が進むとともに、類似した現象が再発した場合の対策を立案するための参考ともなります。

2.2. QNAP 社製の NAS への攻撃を試みるパケットの増加

既に公表されている QNAP 社製の NAS 用ソフトウェアの脆弱性を狙った攻撃が活発化していることを QNAP 社が 6 月 8 日に公[2]にしました。対象となった脆弱性は修正したバージョンが既に公開されています。また、脆弱性の検証コードが研究者によってインターネット上に 5 月 25 日に公開[3]されました。本脆弱性に対する探索や攻撃活動の一端が、TSUBAME のセンサーでは Port8080/TCP 等のパケットとして観測されますが、TSUBAME による観測ではどのような攻撃が意図されているのかまでは分かりません。
どのような攻撃かを確認するために、実証実験中のハニーポットで検証コード公開前の 2020 年 5 月 1 日からのデータを調査したところ、公開された検証コードに見られる特徴が、5 月 27 日以降に観測されたデータ中に確認できました［表 4］。これから、当該脆弱性の探索行為が検証コード公開直後から始まったと言えます。

［表 4：ハニーポットでの観測動向］

観測日	送信元地域	宛先ポート番号	リクエスト	件数
5 月 27 日	ロシア	8080	/photo/p/api/album.php	1
5 月 28 日	ロシア	8080	/photo/p/api/album.php	3
5 月 29 日	ロシア	5000	/photo/p/api/album.php	1
		5001	/photo/p/api/album.php	4
		8083	/photo/p/api/album.php	4
5 月 30 日	ロシア	5000	/photo/p/api/album.php	3
5 月 31 日	ロシア	8080	/photo/p/api/album.php	3

また、［表 4］に掲げたリクエストは、他から得た情報をもとに対象を絞り込んだ上で実施していることも考えられますが、同じ送信元 IP アドレスからの通信が TSUBAME による観測でもほぼ例外なく検知されていることと照らし合わせると、対象を事前に絞り込むことなしに広域を網羅的に探索しているようです。

JPCERT/CC では本脆弱性を対象とした攻撃を受けたとの報告を受領[4]しています。当該製品を使用している場合は、異常がないことをログにより確認することをお勧めします。

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) eCh0raix Ransomware
https://www.qnap.com/ja-jp/security-advisory/QSA-20-02

(3) QNAP QTS and Photo Station 6.0.3 - Remote Command Execution
https://www.exploit-db.com/exploits/48531

(4) QNAP 社製 NAS および Photo Station に影響を与えるランサムウエアに関する情報について
https://www.jpcert.or.jp/newsflash/2020060901.html

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。