JPCERT/CC インターネット定点観測レポート

2020 年 1 月 1 日 ～ 2020 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

2020 年 5 月 12 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。

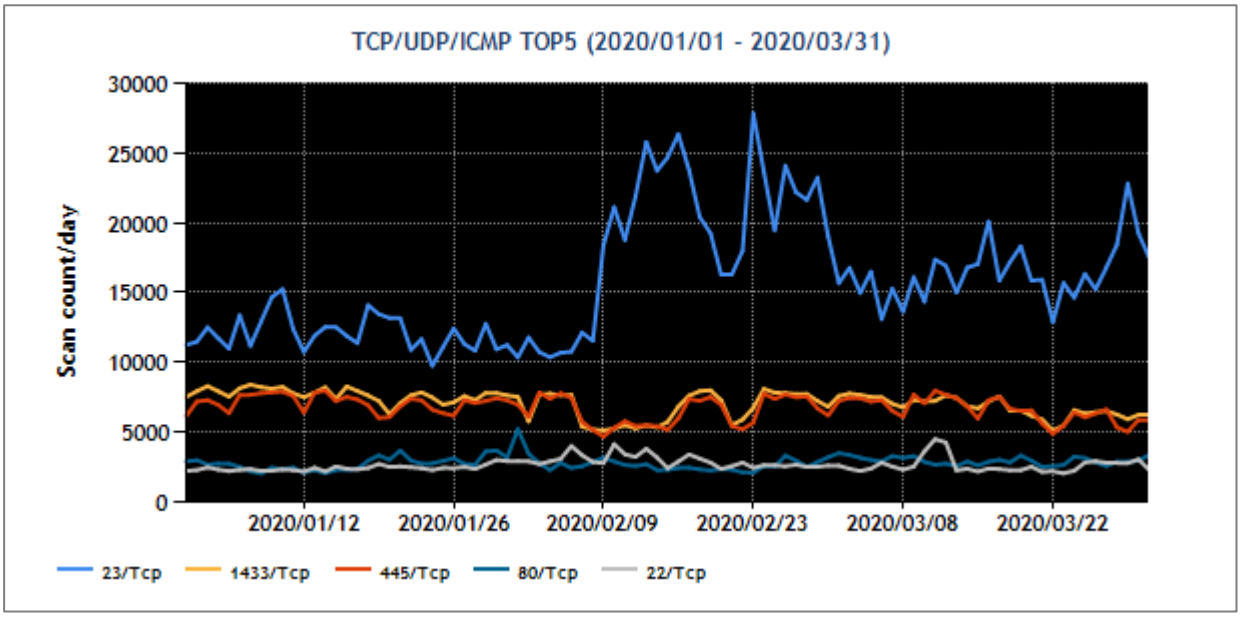
本四半期に国内で観測されたパケットの宛先ポート番号をパケットが多かった順に並べるとトップ 5 は［表 1］に示すとおりでした。

［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	1433/TCP (ms-sql)	3
3	445/TCP (microsoft-ds)	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。



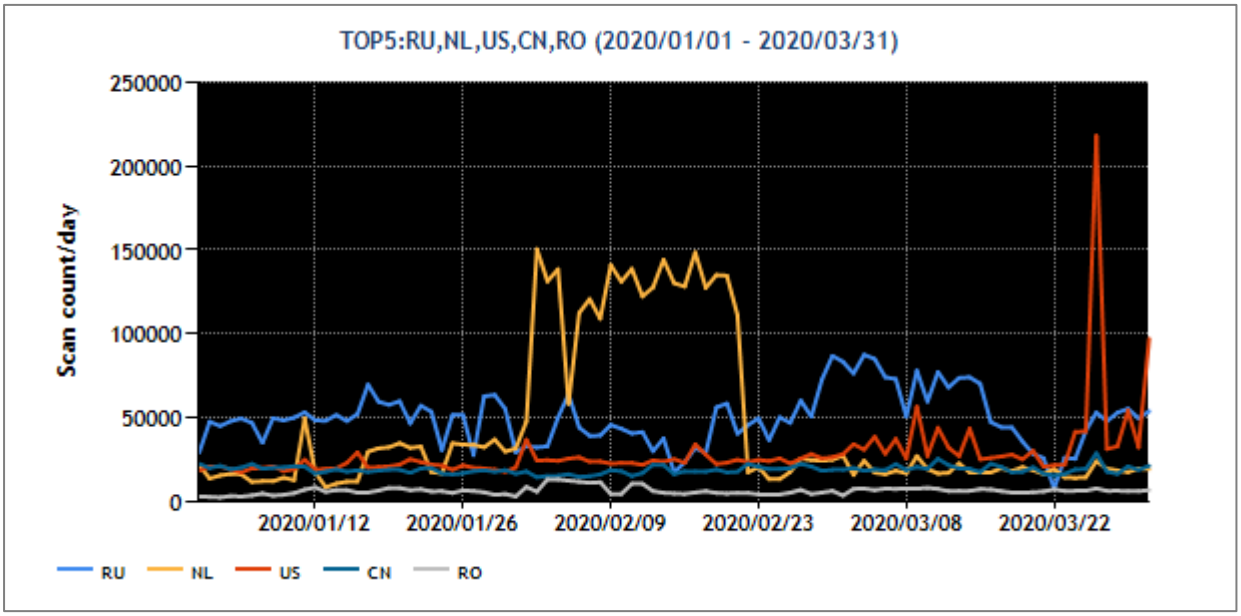
［図 1：2020 年 1～3 月の宛先ポート番号別パケット観測数トップ 5 の推移］

本四半期の期間中、23/TCP 宛のパケットを最も多く観測しました。2 月 9 日頃から約 1 ヶ月間パケット数が多い時期がありました。これは Mirai 亜種等の活動の活発化によるものと推測されます。
前四半期と比較して、445/TCP、1433/TCP 宛のパケットの順位が入れ替わっていますが、445/TCP 宛のパケットの方が減少の波が大きいため、1433/TCP のほうがパケット数として多くなっています。
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	ロシア	2
2	オランダ	1
3	米国	3
4	中国	4
5	ルーマニア	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 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として、TOP5 以外のポート宛のパケットを観測しています。特定のポートの開放ではなく、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. 複数の Citrix 製品の脆弱性(CVE-2019-19781) に対する探索活動について

2019 年 12 月 17 日、Citrix Systems 社が複数の製品に影響する脆弱性の情報[3]を公開しました。本脆弱性に関する実証コード(PoC)も 1 月 11 日頃に公開[4]されました。本脆弱性に対する探索や攻撃活動の一端は、TSUBAME のセンサーで Port80/TCP や Port443/TCP 宛のパケットとして観測されますが、観測結果からスキャン後に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。
どのようなリクエストが送られてくるのかを確認できる実証実験中のハニーポットの 2020 年 1 月 1 日以降のデータを調査したところ PoC に見られる特徴がリクエスト内に含まれていることが確認できました（表 3)。これから、当該脆弱性の探索行為が PoC 公開直後から始まったと言えます。

［表 3：ハニーポットでの観測動向］

観測日時	送信元地域	リクエスト
1月11日15時台	DE	/vpn/%2e%2e/cpns/cfg/smb.conf
1月11日17時台	RU	/vpn/
1月13日1時台	RU	/vpn/../vpns/cfg/smb.conf
1月14日20時台	KR	/vpn/
	KR	/vpn/
	KR	/vpn/
1月15日21時台	US	/vpn/../vpns/cfg/smb.conf

また、［表 3］に掲げた脆弱性の探索は、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[5]しています。脆弱性の影響を受ける当該製品を使用している場合は、攻撃を受けていないことをログにより確認[6]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) NICTER 観測レポート 2019
https://www.nict.go.jp/cyber/report/NICTER_report_2019.pdf

(3) CVE-2019-19781 - Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance
https://support.citrix.com/article/CTX267027

(4) SRemote Code Execution Exploit for Citrix Application Delivery Controller and Citrix Gateway [CVE-2019-19781]
https://github.com/projectzeroindia/CVE-2019-19781

(5) JPCERT/CC インシデント報告対応レポート［2020 年 1 月 1 日～2020 年 3 月 31 日］
https://www.jpcert.or.jp/pr/2020/IR_Report20200414.pdf

(6) 複数の Citrix 製品の脆弱性 (CVE-2019-19781) に関する注意喚起
https://www.jpcert.or.jp/at/2020/at200003.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。