Features of Traffic Generated in the Large-scale Events and Its Impact to the Security Operation

SUDOH Toshiaki

Large-scale international events generate a variety of traffic, including communications related to event operations, communications generated by spectators at the event, and media-related communications such as news coverage and streaming, which have different characteristics from those generated by general organizations and companies. Therefore, in security operations, it is necessary to consider policy definitions, baseline concepts for analysis, and singularity detection methods in accordance with the characteristics of the traffic. This article analyzes the traffic observed during the security operations of the Tokyo 2020 Olympic and Paralympic Games, and discusses its impact on security operations during international events.

Keywords : Tokyo 2020 Games, Network Management, Security Operation, Traffic Analysis, DNS

1. Introduction

We analyze the characteristics of Internet traffic generated from the network related to the Olympic and Paralympic Games Tokyo 2020. We also analyze DNS traffic and discuss the impact of these characteristics on security measures.

2. Traffic Characteristics Analysis

2.1 Time Series Characteristics

Figures 1 and 2 show the traffic volume during the Olympic and Paralympic Games.

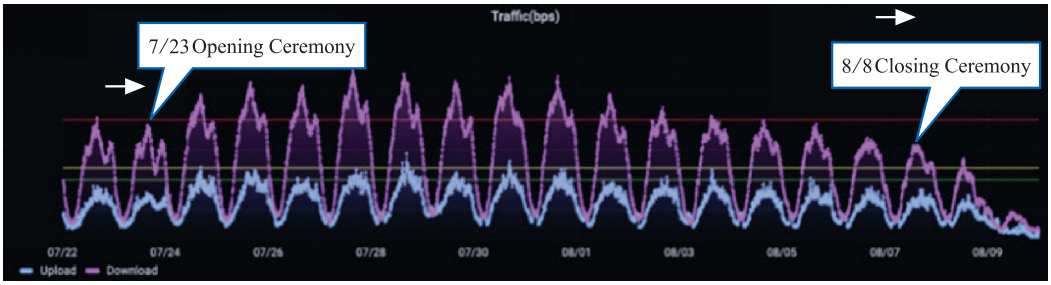
In many events, the peak traffic is observed at the timing of the opening and closing ceremonies, but the Olympic and Paralympic Games do not show any remarkable characteristics, and a saturation curve is drawn about four days after the start of the event, with a peak on the sixth day and a gradual decrease within the estimated traffic range. As shown in Figures 3, the average daily traffic peaked at around 15 : 30, and the second and third highest amounts were recorded at 12 : 00 and 22 : 00 p.m. This is due to the concentration of media-related information and content transmission and reception during these hours. The singularity at around 2 : 00 and the reversal of uplink and downlink traffic amount between 3 : 30 and 5 : 00 are also partially attributable to media-related communications.

2.2 Destination Country

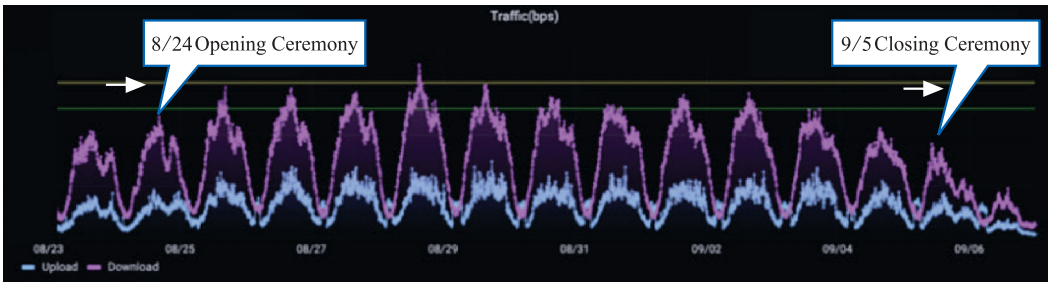
Table 1 shows the percentage of traffic by country.

The U.S. and Japan account for 84.9% and 71.3% of the traffic as a source and destination, respectively, due to the influence of major SNS, CDN, and cloud services. Other common trends were seen in international events where communication with CDNs, media-related and security service providers, etc. were common.

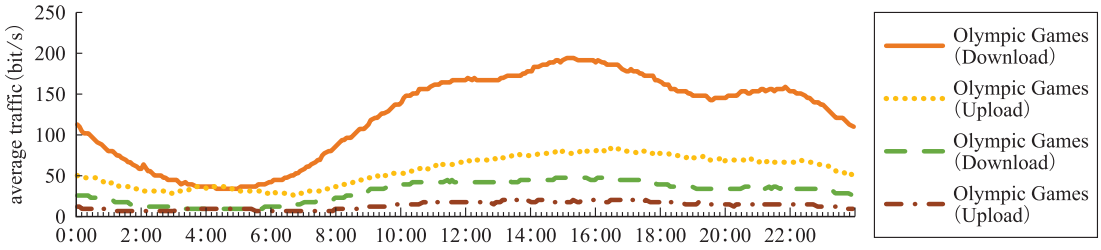
SUDOH Toshiaki
Information Security, NTT Communications Corporation
E-mail t.sudou@ntt.com
The Journal of The Institute of Electronics, Information and Communication Engineers, Vol.105, No.8, Supplement, pp.63-66, August 2022



Figures 1　Traffic during the Olympic Games



Figures 2　Traffic during the Paralympics Games



Figures 3　Average Traffic by Time Period

Table 1　Traffic Volume by Country

Source	%	Destination	%
UnitedStates	45.16%	Japan	49.00%
Japan	39.74%	UnitedStates	22.31%
Singapore	1.89%	Mexico	2.69%
UnitedKingdom	1.65%	UnitedKingdom	2.50%
Netherlands	1.16%	Spain	2.43%
Australia	1.10%	SouthKorea	2.07%
Germany	0.90%	Netherlands	2.06%
Spain	0.82%	Malaysia	1.38%
Russia	0.74%	Singapore	1.36%
France	0.65%	Germany	1.23%
Other	6.17%	Other	12.99%

2.3　Transport Protocol Analysis

Table 2 shows the ratio of send/receive transport protocols.

The ratios of TCP and UDP were very high for both sending and receiving, and the use of other protocols for closed connections, such as GRE and ESP, was negligible.

Table 2 Transport Protocol Ratio

Received			Transmit		
Protocol		%	Protocol		%
6	TCP	63.5060%	6	TCP	52.84489%
17	UDP	36.1982%	17	UDP	46.74986%
1	ICMP	0.2910%	1	ICMP	0.40227%
47	GRE	0.0033%	50	ESP	0.00255%
50	ESP	0.0011%	47	GRE	0.00042%
—	Other	0.0004%	—	Other	0.00001%

Table 3 Communication Port Ratio

No	Receiving Port Number		%	No	Outgoing Port Number		%
1	TCP	443	55.93%	1	TCP	443	49.55%
2	UDP	443	20.77%	2	UDP	443	10.42%
3	TCP	80	5.98%	3	UDP	4500	2.02%
4	UDP	3480	1.54%	4	UDP	2088	1.60%
5	UDP	4500	1.22%	5	UDP	3480	1.55%
6	UDP	3481	0.88%	6	UDP	16393	1.40%
7	UDP	16393	0.59%	7	UDP	40000	1.11%
8	UDP	33001	0.56%	8	TCP	80	1.06%
9	UDP	53	0.41%	9	UCP	6000	0.71%
10	UDP	3478	0.27%	10	—	50	0.64%

2.4 Communication Protocol Analysis

Table 3 shows the top 10 traffic by receiving and sending port number, with TCP443 being the most common, accounting for 55.93% of incoming traffic and 49.55% of outgoing traffic. UDP443 was next, accounting for 20.77% of incoming traffic and 10.42% of outgoing traffic.

SSL communication using TCP443 is used for various purposes, such as Web access and VPN communication, and is one of the factors that increase the percentage. In addition, voice and video distribution, several types of VPNs that use different port numbers, and remote collaboration tools were frequently observed.

3. Analysis of DNS Communication

3.1 Analysis of DNS Resolvers Used

The number of DNS resolvers used during the period was 5315 IPs, and their classification is summarized in Table 4. In this environment, the use of designated DNS is the basic policy, which means that 99.55% of all queries were protected by appropriate DNS security measures. In addition, original security measures such as the use of public DNS, paid Secure DNS, VPN, and Proxy were also observed. We also observed a few cases of malicious DNS use due to the execution of undesirable programs, as well as queries sent to specific DNS resolvers for the purpose of amplification.

Table 4 DNS Resolvers

No	DNS Resolver	Percentage of Total Queries
1	Designated DNS	99.55%
2	Public DNS	0.31%
3	Secure DNS	0.02%
4	VPN/Proxy	0.02%
5	Other	0.10%

We also observed a large number of DoH (DNS over HTTPS) name resolution cases, which also increased TCP443 traffic and may have circumvented normal DNS protection.

4. Summary

The traffic characteristics were less peculiar and more stable than for normal international events. However, there were some unexpected traffic due to changes in the implementation of DoH and other new communications, VPNs, and enhanced endpoint security features such as encryption. Such traffic may circumvent existing

security countermeasures and analysis techniques, and therefore, security operations that combine traffic analysis techniques are required to detect and respond immediately to unexpected traffic.

(Received February 28, 2022, Revised March 7, 2022)

SUDOH Toshiaki

SUDOH Toshiaki graduated from Ehime University in 1995 with a bachelor's degree in electrical and electronic engineering. He joined NTT in the same year. He currently engages in security service development, operation, consulting, etc. at NTT Communications Corporation.