Responding to Cyber Attacks during the Tokyo 2020 Games

ONISHI Masaki　HOSODA Naofumi　NAKANISHI Katsuhiko
IBAYASHI Hiroaki

Abstract

In the past, there were many cyber attacks on the Olympic and Paralympic Games that could affect the operation of the Games. On the Tokyo 2020 Olympic and Paralympic Games, many cyber attacks were observed and reached their peak during the Olympic Games. We describe some representative examples and how we responded to these attacks with the security solutions implemented and the security operations matured during the Games preparation period.

Keywords：Tokyo 2020 Games, Cyber attacks, Security operations

1. Preface

As described in this Special Issue "5-4 Cyber Security Operations for the Tokyo 2020 Games", the Olympic and Paralympic Games Tokyo 2020 (hereinafter referred to as "Tokyo 2020 Games") matured the security operations in preparation for the Games. Cyber attacks were continuously observed since the early preparation period, and the volume peaked during the Games, with a total of 450 million security events observed during the Games.

In this article, we describe representative examples of security responses during the Games and how we responded to cyber attacks and successfully defended the Games.

ONISHI Masaki
Technology Services Bureau, The Tokyo Organising Committee of the Olympic and Paralympic Games
HOSODA Naofumi
Technology Services Bureau, The Tokyo Organising Committee of the Olympic and Paralympic Games
NAKANISHI Katsuhiko
Technology Services Bureau, The Tokyo Organising Committee of the Olympic and Paralympic Games
IBAYASHI Hiroaki
Technology Services Bureau, The Tokyo Organising Committee of the Olympic and Paralympic Games
The Journal of The Institute of Electronics, Information and Communication Engineers, Vol.105, No.8, Supplement, pp.279-284, August 2022
© 2022 The Institute of Electronics, Information and Communication Engineers

2. Security Operation Structure during the Games

The Security Operation Centre (SOC), located within the Technology Operation Centre (TOC) increased staff members and expanded security operation hours one month before the opening ceremony of the Olympic Games. The SOC was in full operation two weeks before the opening ceremony of the Olympic Games, and operated 24 hours a day in three group of a 12-hour shift with a total of approximately 130 staff members (Figure 1). During the Paralympic Games, the number of staff members and operating hours were reduced compared

Figure 1　SOC (©2021-International Olympic Committee-All Rights Reserved)

to those during the Olympic Games.

The SOC received support from the Japan Cybercrime Control Center (JC3) and the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), which dispatched liaison members that served as a point of contact.

During the Games, the security monitoring status was reported and shared at regular daily meetings by members of the International Olympic Committee (IOC), the International Paralympic Committee (IPC), Olympic Broadcasting Services (OBS), Atos SE, NTT Communications Corporation, Nippon Telegraph and Telephone East Corporation, and others.

In Section 3, we describe the security events and incidents observed during the Games and our responses to them.

3. Cyber attacks and Security Responses during the Games

In Section 3, we discuss the significance of numerical values in security operations and the security events observed in the four domains : the Back Office Network (BON) used by the Tokyo Organising Committee members for their work, the Competition Network (CPN) that connected the venues, the Olympic Technology Network (OTN) serving various VLANs dedicated to the Tokyo 2020 Games stakeholders, and the websites located on the Internet (websites). We also describe our security response to the fake live-streaming site dealt with based on the security intelligence.

3.1 Significance of Numerical Values in Security Operations

In security operations, operators check a large number of logs and alerts generated by variety of solutions and classify them into incidents including attacks and false positives that require action, and then respond to them. Actual figures for these logs, alerts, responses, and others are provided here as supplements. Please note, however, that these figures are specific to each domain and environment at the time of the Tokyo 2020 Games, and are not comparable to those of different environments.

The number of attacks itself does not indicate the degree of danger. The number of attacks varies greatly depending on the social conditions, geopolitical risks, attack trends, attacker motivation, and other factors in the host country. The quality and quantity of attacks vary, with some attacks targeting a weak point with minimal accesses, while others, on the other hand, require a large number of accesses over a wide area in order to find a weak point. The number of logs and alerts also varies greatly depending on the implementation and nature of security measures. In recent years, the number of logs and alerts has increased explosively due to the improvement of detection technology, which enables highly detailed detection of risk events, as well as the incorporation of various types of data for advanced analysis of attacks, which is not limited to security. On the other hand, the technology for narrowing down the truly dangerous information from such tremendous information is also becoming more sophisticated, and in many cases, the number of outputs is significantly reduced.

The numerical values vary greatly depending on the nature of the attack and the implementation of security solutions, and the size of the number cannot be used to compare the danger and scale of attacks against different environments, or the strength of security solutions and the adequacy of operational systems.

3.2 450 Million Security Events

Based on the 3.1, Table 1 shows the 450 million security events during the Games. This is a tabulation of the external accesses blocked by the perimeter defense from the number of logs collected for each domain listed in 3.3 to 3.5. This is a numerical index that represents the number of attacks, which is not easily affected by the implementation of solutions, but is not necessarily proportional to the degree of danger.

In the three domains of BON, CPN, and OTN, accesses from outside that are blocked by Unified Threat Management (UTM) or other means are included. The number of detected and blocked attacks that started from routes other than external accesses is not included in the figures in Table 1. In addition, the number of alerts is greatly reduced because only one alert is issued for each series of blocked accesses with a high-risk level. In the Web domain, this applies to accesses blocked by Content Delivery Network (CDN). It is the total number

Table 1 Number of External Accesses Blocked by Perimeter Defenses (Approximate Numbers)

	BON/CPN	OTN	Web	Total Amount
Number of external accesses blocked [cases]	150 million	140 million	160 million	450 million

Table 2　Number of Security Responses in BON

	Olympic Games Period (7.23.2021–8.8.2021)	Paralympic Games Period (8.24.2021–9.5.2021)
Number of security alerts notified by security solutions [cases].	5,808	1,134
Number of reports/inquiries from users and others confirming details of security alerts [cases].	80	70
Number of security incidents affecting staff and systems [cases].	0	0
Reference : Number of logs stored in SIEM* [case].	13,343,465,345	6,863,991,707

*Not all security solution alerts/logs are included. In addition to security logs, logs required for security incident response are also included.

of accesses blocked by three types of filters : rule-based, rate-based, and reputation-based. The details are described in Section 3.5.

3.3　Security Responses in BON/CPN

During the Games, as in the preparation period, we analyzed reports from staff and alerts notified by each security solution, and identified the extent of the impact and causes, which were then addressed (Table 2). During the Games, availability was emphasized, and since the target response time was different between the Games preparation period and the Games, an even faster and more precise response was required.

This section describes an example of a suspicious e-mail sent by a person related to the Games whose e-mail account was compromised, which was detected during the Olympic Games.

In the early morning of August 4, 2021, a suspicious e-mail was sent to seven Tokyo Organising Committee staff members by a person whose e-mail account had been compromised. The suspicious e-mail had an attached file, and when the attached file was opened, a screen that resembled a Microsoft login page was displayed.

All suspicious e-mails were quarantined before they reached the e-mail accounts of the staff members through e-mail security measures, and the staff members did not receive the e-mails. There was no access history for the destinations linked to in the attachments, and the proxy was set to block them, so there was no impact on the Tokyo Organising Committee.

We contacted the organization that the person whose e-mail account was compromised belonged to and asked them to take action. We also shared the case with the intelligence sharing platform which the IOC established to share information among the Tokyo 2020 Games stakeholders, and alert them to the situation.

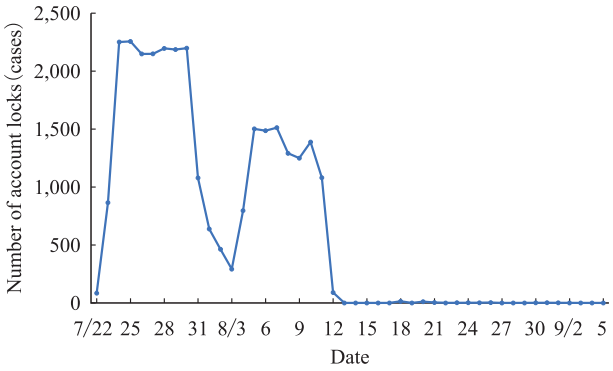

Figure 2　Number of Account Locks in Azure AD

As another example, we describe a security event for the Tokyo Organising Committee accounts. Figure 2 shows the number of account locks observed in Azure Active Directory (Azure AD), a Microsoft authentication service used by the Tokyo Organising Committee. The account lock function was set to lock the account for a predetermined time after a predetermined number of consecutive password authentication failures. As shown in Figure 2, a large number of account locks occurred from July 23, 2021, the day of the opening ceremony of the Olympics while almost none occurred during the Paralympic Games. Analysis of the accounts that were locked showed that the source IP addresses were almost all connections from overseas, with five countries accounting for about half of the total number of account locks.

Since account locking was not implemented to prevent legitimate use, there was no impact on business operations. We confirmed that no unauthorized access occurred based on the attack analysis originating from the accounts that were locked. In addition, since the Tokyo Organising Committee used two-factor authentication for all authentication, it was difficult for unauthor-

Table 3 Number of Security Responses in OTN

	Olympic Games Period (7.23.2021–8.8.2021)	Paralympic Games Period (8.24.2021–9.5.2021)
Number of security alerts notified by security solutions [cases].	5,287	772
Number of reports/inquiries from users and others confirming details of security alerts [cases].	92	29
Number of security incidents that were analyzed and blocked or otherwise addressed [cases].	12	13
Reference 1 : Total number of security solution logs [cases].	70,878,430	90,432,424
Reference 2 : Number of OTN connected clients [units]. (Unique, daily cumulative total)	1,429,149	578,435

* It is unknown whether users and systems were actually affected or not, since terminals/systems connected to OTN are brought by users.

ized access to occur due to password leakage, and passwords were reset for all staff members immediately before the Games. The risk of this security event was low.

3.4 Security Responses in OTN

We responded to security events and incidents such as port scans and vulnerability scans from external sources and malware infection of PC terminals brought in by the Tokyo 2020 Games stakeholders. Table 3 shows the number of security events and incidents handled. No security incidents occurred on the Tokyo Organising Committee-managed PCs and IT systems deployed in OTN.

Focusing on the figures of Reference 1 and Reference 2 in Table 3, the number of logs was higher during the Paralympic Games than during the Olympic Games, even though the number of connected terminals was smaller during the Paralympic Games. We assume that this is because the detection function continued to be improved and added as new attack information became available during the Games, enabling more detailed monitoring and increasing the number of logs generated in the later stages of the Games.

We describe an example in which an attacker targeted a vulnerable IT environment built by a Tokyo 2020 Games stakeholder and exploited it as a stepping stone. The organization was using the Internet connection with a global IP address. As a result of detecting and analyzing suspicious communications from the global IP address, it was found that the system brought in by the organization was in an open proxy state, allowing any user to connect from the Internet, and was being used to relay communications to phishing sites and malware sites and to relay spam mail. We contacted the organization that owned the system and asked them to take action, and also took measures using the UTM deployed in OTN.

In addition, with the cooperation of the National center of Incident readiness and Strategy for Cybersecurity (NISC), the National Institute of Information and Communications Technology (NICT), JC3, JPCERT/CC, ICT-ISAC Japan (ICT-ISAC-J), and security vendors, we detected the open resolvers with improperly configured Domain Name System (DNS) settings, the use of outdated software with vulnerabilities, and the state in which the management screen of the system was accessible from the Internet, etc. We also contacted the organization that owned the system and ask them to take action.

The combination of various monitoring methods, such as Threat Hunting and external monitoring, is important for the early detection of such cases. As an example of this, we describe in this special issue "5-6 Find Evil-Know Normal : Tokyo 2020 Games Threat Hunting from Internal and External Perspectives" and "5-7 Impact Analysis of Cyberattacks to the Critical Sites by External Monitoring".

3.5 Security Responses on the Websites

At the past Games, attacks on websites increased rapidly around the time of the opening ceremony of the Games. The Figure 3 appears to be different from those in Figure 6 of "3-9 Tokyo 2020 Games-Time Official Website and Mobile Application" in this special feature, this is due to the difference in the units used for the aggregation. In the "Tokyo 2020 Games—Time Official Website and Mobile Application", the figures are based on the number of page views from the perspective of analyzing user trends, while in this article, the figures

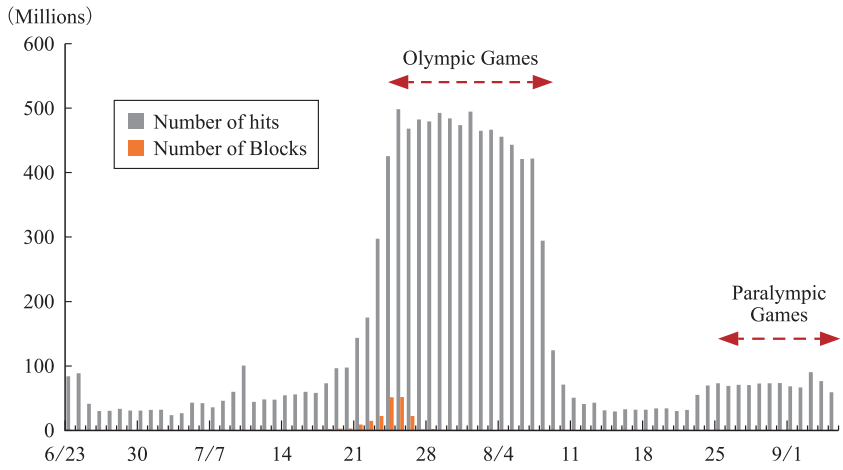

Figure 3　Number of Blocked Websites

Table 4　Number of Security Responses on the Web

	Olympic Games Period (7.23.2021-8.8.2021)	Paralympic Games Period (8.24.2021-9.5.2021)
Number of accesses blocked [cases].	160,129,766	3,618,826
Number of security alerts notified by security solutions [cases].	10,631	6,266
Number of reports/inquiries from users and others confirming details of security alerts [cases].	498	340
Number of security incidents affecting staff and systems [cases].	0	0
Reference : Number of logs stored in SIEM* [case].	1,050,662,927	292,163,428

*Not all security solution alerts/logs are included.

are based on the number of accesses from the perspective of analyzing the content of access. Both of the numbers of blocks are based on the number of blocked accesses. Although accesses to official Web sites dominated the number of blocked accesses, a considerable number of accesses were also made to other sites. The content of these blocked accesses was to access a group of web domain sites at high frequency for several hours to check for the use of vulnerable software or inappropriate settings. Although we observed such accesses frequently before and after the opening ceremony, they were typical attacks for known vulnerabilities rather than accesses based on the characteristics of the Tokyo 2020 Games website, and because the frequency was unusually high and included many widely known attack methods, they could be easily blocked by rate-based and rule-based filters. Some of them repeatedly requested specific content and may have intended to overload the service, but these were also easily detected and quickly blocked by the rate-based filter, and did not adversely affect the service. These source IP addresses varied, and were not characterized by a specific country, region, or providers.

In addition to these, there were many small-scale suspicious accesses, but both the quality and quantity were similar to those seen in the period before the start of the Games, and they were not unique and could be blocked by the rule-based and reputation-based filters.

Table 4 summarizes the number of alerts and security responses in the Web domain. In the architecture adopted in our operation, a series of unauthorized accesses are combined into a single alert.

Attacks on Web systems are often carried out using vulnerabilities as a foothold. In any case, whether these accesses were intended as attacks or not, it was very important to protect the Games by preventing them in the preliminary investigation phase.

3.6　Security Response from Security Intelligence

While monitoring information provided by the Security Intelligence Service and similar domains under the name of the Tokyo 2020 Games, we detected sites that pretended to be live-streaming sites for the Torch Relay, the Olympic Opening Ceremony, and various

competitions, etc.

There were three main types of methods used to access fake live-streaming websites. After a user accesses the fake live-streaming site, the following cases were observed:

(1) A case in which the user is led to a spam site that abuses browser notifications.
(2) A case in which the user is asked to sign up for a paid VPN service.
(3) A case in which the user is asked to enter credit card information.

In particular, we observed a rapid increase in the number of similar fake live-streaming sites a few days before the opening ceremony of the Olympic Games. On the day of the opening ceremony, we confirmed that users were transferred to the fake live-streaming site from a legitimate domain of Japanese company. We also confirmed that users were being directed to the fake live-streaming website through fake official accounts on YouTube (a video distribution site) and Twitter (a social networking service).

NISC, JC3, JPCERT/CC, and security vendors also detected similar fake live-streaming sites. We asked each organization to provide us with information on fake live-streaming sites they detected. Then we cooperated with external organizations such as security vendors to register the sites with the anti-phishing function of the browsers and to take down the sites. In total, we detected and responded to more than 400 fake live-streaming sites.

4. Conclusion

We described the cyber attacks observed during the Games and the responses to them. During the Games, we observed cyber attacks from outside and internal attacks caused by devices brought in by the Tokyo 2020 Games stakeholders, but we were able to successfully defend the Games without any security incidents affecting the Games operations.

In retrospect, however, the efforts made during the Games preparation period were just as important as those made during the Games. The significance of the period for operational maturity was described in this Special Issue "5-4 Cyber Security Operations for the Tokyo 2020 Games". An even more important factor in the success of stable operations during the Games was that no vulnerabilities were left behind during the Games preparation period and left no foothold for attacker to penetrate the system. The number of attacks peaked during the Games, but the degree of danger is not proportional to the number of cyber attacks. During the preparation period for the Games, we not only responded to security incidents such as suspicious e-mails and vulnerabilities within the Tokyo Organising Committee, but also detected site defacements and e-mail account compromises of the Tokyo 2020 Games stakeholders, and responded in cooperation with the Tokyo 2020 Games stakeholders, and took a series of appropriate measures without missing events that could have served as footholds for attacks, which resulted in ensuring security during the Games.

(Received February 28, 2022; Revised March 16, 2022)

ONISHI Masaki

ONISHI Masaki was engaged in security management at NTT Communications Corporation. He has been seconded to the Tokyo 2020 Organising Committee as the Director of Security Operation, Cyber Security Department, Technology Services Bureau since 2018. During the Games, he was responsible for the security incident response at the SOC.

HOSODA Naofumi

HOSODA Naofumi has been working for ISP backbone operation and analysis of cyber threats at NTT Communications Corporation. He has been seconded to the Tokyo 2020 Organising Committee as Security Operations Manager of the Cyber Security Department, Technology Services Bureau since 2014. During the Games, he was in charge of web security operations at the SOC.

NAKANISHI Katsuhiko

NAKANISHI Katsuhiko was engaged in security incident response and cyber exercise at NEC Nexsolutions, Ltd. and has been seconded to the Tokyo 2020 Organising Committee as the Director of Cyber Attack Response Department, Security Bureau, and Cyber Security Department, Technology Services Bureau since 2015. During the Games, he was responsible for the overall security operations at the SOC.

IBAYASHI Hiroaki

IBAYASHI Hiroaki has been working in the service development of cloud and security businesses at NTT Communications Corporation since 2014, and has been seconded to the Tokyo 2020 Organising Committee as the Director of Cyber Security Department, Technology Services Bureau. During the Games, he was responsible for the overall security operations in the SOC.