Impact Analysis of Cyberattacks to the Critical Sites by External Monitoring

SUDOH Toshiaki

Abstract

During large-scale international events, cyberattacks by attackers with various agendas occur everywhere, from the real world to the Internet, and have a significant impact on the event itself and its stakeholders. Attack targets are not limited to the direct event environment, but also include important sites of the host country, the host municipality, sponsors and other related companies, and various critical infrastructures such as transportation, communication, and electricity. This article analyzes the external monitoring of the Olympic and Paralympic Games Tokyo 2020 related sites and its results, and discusses effective monitoring methods.

Keywords : Tokyo 2020 Games, Network management, Security, Alive monitoring, Port scan

1. Introduction

To monitor the heath and quality of a system, it is more efficient to conduct external monitoring, in which the system is actively checked from the user's point of view from the outside, than passive methods such as log analysis. The same applies to detecting the damage and impact of cyberattacks. In this report, we discuss the results of monitoring by the following two systems :

（１） Critical site monitoring using a decentralized external monitoring system

（２） Port scanning by a wide-area scanning system

2. Decentralized External Monitoring System

2.1 Monitoring Methodology

The purpose of website monitoring is to confirm availability and quality among other aspects. However, when some abnormality is detected, the cause may vary widely, such as access concentration, maintenance, and network failure. Therefore, it is necessary to monitor the website for cyber-attacks in order to grasp the impact of cyberattacks promptly. Therefore, we added a function to quickly identify the effects of cyberattacks and conducted monitoring.

2.1.1 Elimination of Monitoring Environment Dependency

By connecting multiple agents to multiple network services for monitoring, environmental dependence of monitoring agents can be eliminated and the scale of impact can be estimated through simultaneous detection.

2.1.2 Correlation with Cyberattack Trigger Information

By analyzing attack threats posted on SNS and attack information obtained through malware analysis, the possibility of an attack occurring on a monitored target can be traced.

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.288-290, August 2022

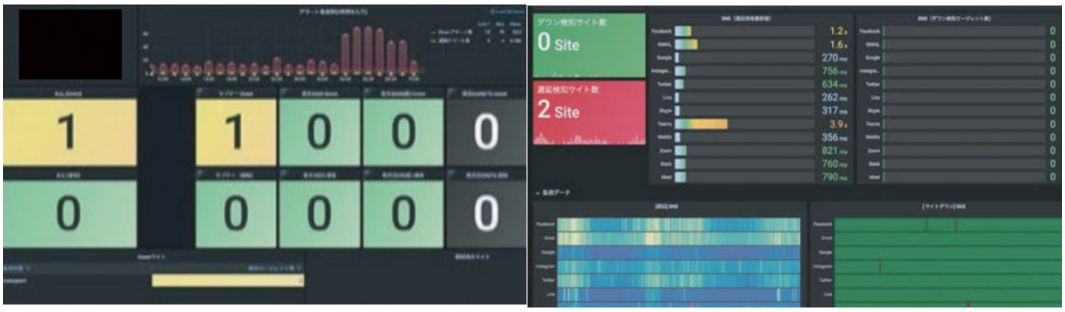

Figure 1　Example of Monitoring Screen

2.1.3　Correlation with Attack Occurrence Information

The occurrence of Distributed Denial of Service (DDoS) attacks, in which a large amount of traffic is sent from multiple computers to a target website or server by honeypots and traffic analysis to make the service unavailable, is confirmed and a correlation analysis is performed. Check the occurrence of DDoS attacks, and perform correlation analysis.

2.1.4　Others

A dashboard as shown in Figure 1 will be prepared for monitoring information, and Chatbot will be used for notifications. Automatic operation is also performed to check the alerted information, and the results of secondary analysis are automatically notified via Chatbot.

2.2　Monitoring Results

We selected 48 sites related to the convention, as well as 489 important sites in Japan, including government agencies, public organizations, telecommunications, broadcasting, electric power, transportation, Internet service providers, SNS services, and streaming services, which are vulnerable to attacks and may be affected. As a result, we detected six attack threats, six cases of unstable communication after detecting an attack, and two cases of failure of the Content Delivery Network (CDN) service used by the websites for efficient content delivery during the period. Most of the cases were detected within several tens of minutes, and the longest was about two hours, and the service itself was not affected.

3.　Wide-Area Scanning System

Next, information related to the event-related network was extracted from the results of the wide-area scanning system across Japan and was analyzed.

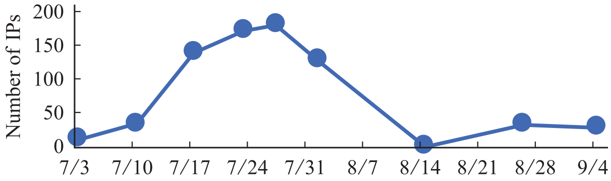

Figure 2　Number of IPs Responding

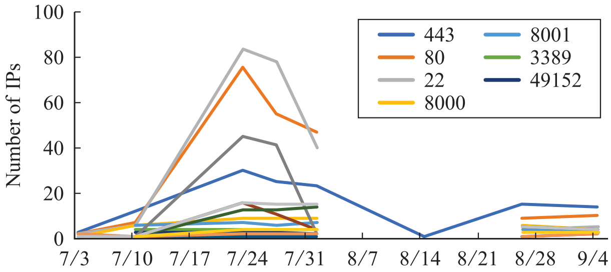

Figure 3　Trends in Response Port Numbers

3.1　Consideration of the Number of Responding IPs and Port Numbers

Figure 2 shows the number of IPs with at least one port reachable via the Internet. The number of unique IPs detected during the period was 239, with a daily maximum of 179.

Figure 3 shows the number of response port numbers during the Olympic period, and Table 1 shows a list of port numbers. As the number of users increased, many undesirable ports including TCP22 (ssh) and TCP23 (telnet) began to return responses, but both the number of responding IPs and port numbers gradually decreased as corrective measures were taken.

Table 1　Top 10 Response Port Numbers

No.	Port No.	Service Name	Number of IPs
1	80	http	111
2	22	ssh	94
3	53	dns	48
4	443	https	45
5	23	telnet	20
6	8080	http alt	17
7	9002	Unknown	17
8	554	Rtsp	16
9	1935	Rtmp	16
10	8000	Unknown	13

Table 2　Equipment Estimation

No.	Device Estimation	Number of IPs
1	Voice Encoder	113
2	Wireless Access Points	64
3	Routers	8
4	Printers	2
5	Firewall	2
6	Server	8
7	Other	113

3.2　Estimation of Connected Devices

It is possible to estimate the connected devices not only by the simple port open status, but also by the banner information sent in response. Table 2 shows the estimated connected device information. Many events detect a large number of responses from audio and video devices, and audio encoders were detected most frequently in the Tokyo 2020 Games as well. In addition, printers and wireless access points were also detected. Since login prompts are also displayed, security measures and vulnerability diagnostics for special devices used in such events need to be considered.

4.　Conclusion

In this article, we have developed a distributed external monitoring system and a wide-area scanning system with additional functions and adjusted for cyberattacks. The monitoring and investigation functions of these systems functioned effectively, and led to improved speed and accuracy of various security operations from a broad perspective, including the impact on sites directly or indirectly related to the event. In order to further improve responsiveness, we aim to achieve even more accurate security monitoring and operations by taking an approach that enhances correlation between synthetic monitoring, which mimics user behavior, and even more security intelligence.

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

SUDOH Toshiaki

Toshiaki Sudoh 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.