Find Evil-Know Normal : Tokyo 2020 Games Threat Hunting from Internal and External Perspectives

HATADA Mitsuhiro　SUDOH Toshiaki

Abstract

The Olympic and Paralympic Games Tokyo 2020 see a significant increase in the number of users and devices prior to the opening of the Games, and the threats to systems vary accordingly. In addition, not only systems strictly controlled by security solutions but also those simply connected to the Internet exist. In order to prevent the occurrence and spread of damage in such an environment, we present case studies of threat hunting based on log analysis inside a network and traffic analysis at the Internet gateway from various perspectives, and discuss prospects of threat hunting for future events.

Keywords : Threat hunting, Log analysis, Traffic analysis, Intelligence

1. Introduction

"Find Evil-Know Normal"[1] is a phrase that is truly realized when threat hunting is conducted to search for threats in a cross-sectional and combined manner using all logs of network devices, terminals, and various security measures, as well as the intelligence collected. High-impact attacks target organization-specific vulnerabilities using organization-specific tools and techniques, so public information and simple Indicator of Compromise (IoC) are not highly effective.

Threat hunting is a search activity that proactively detects threats that have been overlooked by conducting security monitoring and analysis, including the development of custom IoCs and tools. Because it relies on the premise that existing security measures cannot detect attacks with truly high impact. When a breach has already occurred, the objective is to minimize damage by shortening the latent period. It is necessary to suspect the failure of detection caused by both functions and operations of devices, configurations, log collection and analysis, and visualization. Then, making continuous improvements could be another objective of threat hunting.

2. Threat Hunting Based on Log Analysis

In the network of the Olympic and Paralympic Games Tokyo 2020 (hereinafter referred to as "Tokyo 2020 Games"), the policy is to allow only necessary communication between segments. In terms of policy violations, we present two cases in which firewall block logs between segments were investigated.

We found approximately 2.24 million blocked logs per day from a large number of source IP addresses in a specific segment, directed to a specific destination IP address and port number. This had been occurring for several weeks, and the number of blocked logs was

HATADA Mitsuhiro (IEICE Member)
Information Security, NTT Communications Corporation
E-mail mitsuhiro.hatada@ntt.com
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.285-287, August 2022

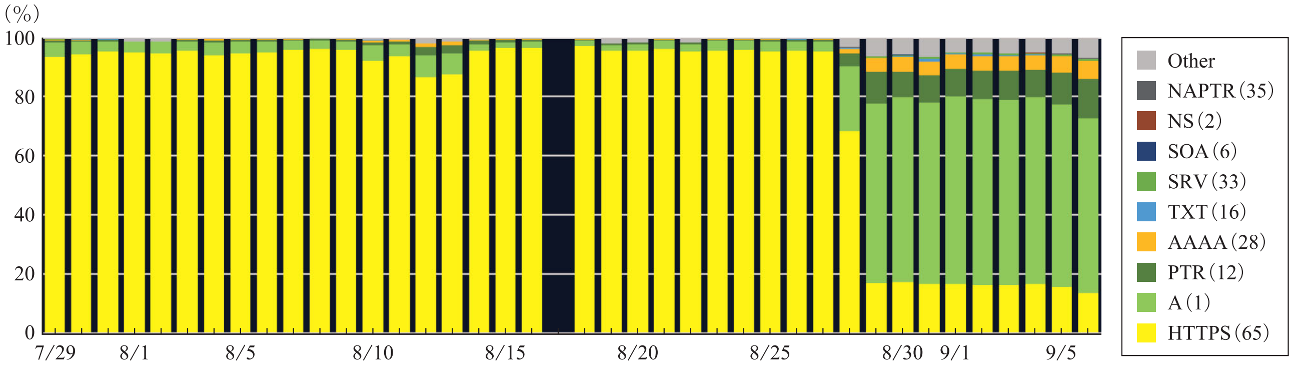

Figure 1 Daily Ratio of DNS Query Type

increasing day by day. As a result of the investigation by the partner, a server that backs up the data of a certain system was deployed before the opening ceremony of the Olympics. Then the client application with an incorrect setting of IP address as a backup server was distributed to user terminals. This is a case where threat hunting contributed to the improvement of system availability in terms of communication failure and overload on SIEM (Security Information and Event Management) caused by a large number of unnecessary logs.

In another case from the perspective of detecting suspicious behavior, we investigated terminals where a set of commands were executed within a few minutes which are commonly used by attackers[2]. A certain application was executing ipconfig, netstat, ping, and tracert as child processes, which looked suspicious. But the results of the sandbox analysis showed that it was legitimate behavior. As a SIEM analyst, we also investigated from various perspectives, such as domains where only one user was accessing the web site (unique behavior of user) and traffic between legitimate users and IP addresses that attempted to log in to Azure AD (communication with the attack source). Finally, there was no evidence of the breach.

The most important point in conducting log analysis-based threat hunting is, “As the environment changes, so do the logs. As the logs change, so does the threat hunting.” It is also effective to search for traces of attacks by relaxing the detection conditions of individual security measures and SIEM’s detection logic. It is also crucial to accumulate patterns to be excluded and prioritize others based on the investigation time and number of cases.

3. Traffic Analysis-based Threat Hunting

In this section, we present a case study of traffic anomaly analysis that detected a large number of ICMP port unreachable messages. We initially assumed that it was a response to a port scan or a DDoS attack, but traffic analysis revealed that it was a large number of DNS responses with a response code of “REFUSED.” The DNS request type analysis revealed that HTTPS RR (Type 65) queries accounted for 95% of all queries, as shown in Figure 1. Secure DNS service, which is the DNS resolver deployed in this environment, does not support HTTPS RR (Type 65), so all of them returned with REFUSED responses. In addition, since a large number of queries and query responses were being transferred, it is assumed that a large number of ICMP port unreachable messages were being sent due to abnormal packet processing by NAPT and firewalls.

At that time, only OS X sent HTTPS RR (Type 65) queries by default, and it is assumed that many OS X users were connected. Although this case is not a security incident directly, the unintentional and chain of large-volume traffic may overload devices such as firewalls with overflowing sessions. Furthermore, it may result in missing logs, DoS effects such as communication failure. In the worst case, the security level may be lowered by bypassing the security function.

In traffic analysis-based threat hunting, we detected vulnerable devices being attempted to log in or execute remote commands, malicious traffic aimed at infection spread or DDoS attacks, and anomalous packets attempting to enter from the outside. We also conducted a deep analysis escalated by other analysis teams. In total, 206 cases were handled throughout the period, and no major damage was confirmed. By leveraging a variety of external threat intelligence, our observation data, and research results, we were able to hunt threats that were overlooked by external traffic analysis rather than relying solely on device logs and alerts. Even if the security measures are sufficient, the external traffic analysis approach is effective not only in detecting anomalies, but also in determining whether the network is in a normal state.

4. Summary

The number of users and devices increased significantly prior to the opening of the Tokyo 2020 Games. With these changes, the threats to which systems are exposed have also diversified. In addition, there was a mixture of systems that can be strictly managed by security solutions and those that just use Internet access. In order to prevent the occurrence and expansion of damage in such environments, this article presented case studies of threat hunting conducted from multiple perspectives, including log analysis of various systems and internal networks, and external traffic analysis at the Internet gateway. These cases and lessons learned can be applied not only to future large-scale events but also to the organization network.

References

（1） SANS Institute, Hunt Evil Poster, 2021.
https://www.sans.org/posters/hunt-evil/

（2） S. Tomonaga, Windows Commands Used by Attackers, JPCERT/CC, 2021.
https://blogs.jpcert.or.jp/ja/2015/12/wincommand.html

（Received February 28, 2022 ; Revised March 1, 2022）

HATADA Mitsuhiro（IEICE Member）

Dr. Hatada is currently a director of Security Operation, Information Security, NTT Communications Corporation. He received his B.E. and M.E. degrees in computer science and engineering, and Ph.D. in engineering from the Waseda University in 2001, 2003 and 2018, respectively. He joined NTT Communications Corporation in 2003 and has been engaged in the research and development of applied security.

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.