Cyber Threat Report of The 9th Asian Winter Games Harbin 2025

April 2025

National Computer Virus Emergency Response Center
National Engineering Laboratory for Computer Virus Prevention Technology

April 3rd, 2025

Executive summary

The 9th Asian Winter Games were held in Harbin, Heilongjiang Province, China from February 7 to February 14,2025 and was a complete success. While this important event has received wide attention at home and abroad, it has also become the target of cyber attacks. This report comprehensively summarizes cyber security threats monitored and handled by the cyber security team during the event. Relevant statistics show that during the competition, the information systems of competition and the critical network infrastructures in Heilongjiang province were attacked by a large number of network attacks from abroad. Most of the attacks came from the United States, the Netherlands, Singapore and other countries and regions. Under the active joint efforts of the cyber security team, these cyber attacks failed to have a serious impact on the event. However, it further highlights the severe situation of China's network suffering from frequent overseas attacks.

1 Cyber Attacks target Information Systems of Competition(ISCs)

Overview

According to the analysis and data statistics of the logs of the ISCs during the event, from January 26 to February 14,2025, the number of cyber attacks from abroad was 270,167 times. The number of attacks increased significantly from February 7 to February 13, reaching the peak on February 8.

Attacks on the ISCs

Starting from January 26, the cyber security team launched a joint investigation and emergency response work, banning the IP addresses of overseas attack sources identified as high-risk, to ensure that the data interaction between the ISCs operates in a safe and reliable environment. Monitoring data show that since the opening of the first ice hockey game on February 3, the abnormal network traffic such as network asset discovery and massive port scanning to the ISCs has continued to increase, accompanied by a large number of exploitation attempts.

The attacks targets multiple ISCs, among which the three systems with the largest number of attacks are the information service system, the arrival and departure management system and the charging card system. Many kinds of attack behaviors were detected, including network

assets discovering and malicious port scanning, exploiting the known system vulnerabilities or injection vulnerabilities of Web system to implement penetration. At the same time, the TTPs (Tactics, Techniques & Procedures) reflects that the attacker's intention to directly attack on the ISCs is quite clear.

Among the sources of identified attacks, the United States carried 170,864 attacks, accounting for 63.24%. It was followed by Singapore (40,449 times, accounting for 14.97%), the Netherlands (12,414 times, accounting for 4.95%), Germany (6,682 times, accounting for 2.47%), Republic of Korea (1,281 times, accounting for 0.47%) and other countries and regions.

The mainly attack types are Web attacks, including arbitrary file read vulnerability exploitation, SQL injection attacks, HTTP X-Forwarded-For spoofing, etc.

Banned IP addresses

According to statistics, during the event, the cyber security team has banned 12,602 high-risk malicious IP addresses overseas. These malicious IP addresses are maliciously scanned and exploited against the ISCs, intending to invade and steal the system data or directly damage the system, most of which come from Digital Ocean cloud service hosts.

2 Cyber Attacks target Critical Network Infrastructures in Heilongjiang Province

From January 31 to February 14, the cyber attacks on critical network infrastructures in Heilongjiang province came mainly from the United States and its Allies. Statistics show that during this period, the top 3 numbers of times of attack from the Netherlands (37.98 million times), United States (11.79 million times), and Thailand (7.2 million times). Australia, the United Kingdom, Germany, Lithuania, Canada, Japan and Singapore, in turn, ranked fourth to tenth, see Appendix I for details.

According to the number of attacks initiated by single overseas IP address, the IP address from the Netherlands (193.142. *. *) ranked first with 3,25,20,351 attacks, multiple IP addresses located in the United States carry out cyber attacks on critical network infrastructure in Heilongjiang Province. Although the number of attacks from a single IP address is less than the above Netherlands IP address, but the total number of attacks is relatively high, see Appendix II for details.

3 Conclusion

The comprehensive analysis of cyber attacks on the information systems of the Asian Winter Games and critical network infrastructures from overseas shows that, the attacks from the United States, Netherlands and some other countries and regions are relatively intensive. And,

it is worth noting that in January 2025, the National Computer Network Emergency Response Technical Team/Coordination Center of China has released the investigative reports[1] show recent cyberattacks on Chinese tech firms by the U.S., and the report also told that the United States frequently used cloud hosts located in the Netherlands, Germany and other European countries as a hop or puppet host. In this regard, the cyber security team conducted a attribution analysis of these attacks. Based on the TTPs, timeline, timezone, language and other behavioral characteristics, cyber security team highly suspected that the cyber attacks on ISCs and the critical network infrastructures in Heilongjiang during the Asian Winter Games were related to the United States government.

The situation above shows that during the hosting of large-scale international sports events in China, foreign hostile forces spare no effort to destroy and interfere with the normal operation of the sports events through cyber attacks, and even try to create chaos and steal sensitive information by attacking critical network infrastructures in China. We strongly condemn such malicious cyber attacks against international civilian exchanges activities, and we will submit the details and artifacts of these attacks to the public security sector.

[1] https://www.cert.org.cn/publish/main/49/2025/20250117141608670773438/20250117141608670773438_.html

Appendix I

Top 10 Countries of Attack Source

Rank	IP Location	Times of Attack
1	Netherlands	37983182
2	United States	11798655
3	Thailand	723451
4	Australia	382540
5	United Kingdom	328726
6	Germany	233509
7	Lithuania	189071
8	Canada	168270
9	Japan	97572
10	Singapore	63390

Appendix II

Top 10 IP addresses of Attack Source

Rank	IP	IP Location	Times of Attack
1	193.142.*.*	Netherlands	32520351
2	204.76.*.*	United States	952981
3	204.76.*.*	United States	391062
4	83.164.*.*	Austria	287506
5	98.197.*.*	United States	261124
6	98.197.*.*	United States	253287
7	98.197.*.*	United States	250986
8	98.197.*.*	United States	250973
9	98.197.*.*	United States	250551
10	98.197.*.*	United States	247645