



“2025 年哈尔滨第九届亚冬会” 赛事信息系统及黑龙江省内关键 信息基础设施遭境外网络攻击 情况监测分析报告



〔内容摘要：第9届亚洲冬季运动会于2025年2月7日至2月14日在中国黑龙江省哈尔滨市举行并取得圆满成功。本届重要赛事在得到国内外广泛关注的同时，也成为网络黑客攻击的目标。本报告全面总结了网络安全保障团队监测处置的本届赛事各类网络安全威胁情况。相关统计数据表明，赛事期间，各赛事信息系统、黑龙江省域范围内的关键信息基础设施遭到来自境外的大量网络攻击。攻击源大部分来自美国、荷兰等国家和地区。在赛事网络安全保障团队的共同努力下，这些网络攻击未能对赛事造成严重影响，但却进一步凸显了我国网络频繁遭受境外攻击的严峻形势。〕

一、亚冬会赛事信息系统遭境外网络攻击情况

（一）网络攻击总体态势

赛事网络安全保障团队对亚冬会网络及赛事信息系统网络日志全面开展复盘分析，发现自2025年1月26日至2月14日期间，亚冬会赛事信息系统遭到来自境外的网络攻击270167次。网络攻击数量呈波动性增长态势，2月7日至2月13日攻击次数显著增高，其中2月8日达到攻击次数峰值。

（二）赛事信息系统安全监测情况

从1月26日开始，网络安全保障团队启动联合研判和应急处置工作，对判定为高危的境外攻击源IP地址实施封禁，确保不同场馆之间赛事信息系统的数据交互在安全可靠的环

境中运行。监测数据表明，自 2 月 3 日第一场冰球比赛开赛以来，针对赛事信息系统的网络资产探测与批量端口扫描等网络异常行为流量持续增加，同时伴随有大量漏洞利用攻击事件。

1.攻击对象及行为分析

网络攻击针对多个赛事信息系统展开，其中，遭受攻击次数最多的 3 个系统分别为赛事信息发布系统、抵离管理系统和收费卡系统。网络攻击行为主要是通过探测扫描获取相关网络资产的指纹信息，并利用已知系统漏洞或 Web 系统注入漏洞实施入侵。攻击过程及攻击手法反映出攻击者对赛事信息系统的攻击意图较为明确。

2.境外攻击源分布情况分析

在被识别出攻击中，来自美国的攻击次数为 170864 次，占比高达 63.24%；其次是新加坡（40449 次，占比 14.97%）、荷兰（12414 次，占比 4.95%）、德国（6682 次，占比 2.47%）、韩国（1281 次，占比 0.47%）等国家和地区。

3.网络攻击类型分析

此次遭受的网络攻击以 Web 攻击为主，具体包括文件读取漏洞攻击、SQL 注入攻击、HTTP 协议头 X-Forwarded-For 字段伪造攻击等。

（三）IP 封禁情况分析

据统计，亚冬会期间共封禁高危恶意 IP 地址 12602 个，

这些恶意 IP 地址针对赛事信息系统进行恶意扫描、漏洞利用操作，意图入侵并窃取信息系统数据或直接对信息系统实施破坏，其中大部分攻击来自境外 Digital Ocean 云服务主机。

二、黑龙江省内关键信息基础设施遭受境外攻击情况

1 月 31 日至 2 月 14 日期间，针对黑龙江省内关键信息基础设施实施的网络安全攻击主要源自美国及其盟友国家，其中攻击次数最多的三个国家分别为荷兰（3798 万次）、美国（1179 万次）、泰国（72 万次）。澳大利亚、英国、德国、立陶宛、加拿大、日本和新加坡分别位列第四至第十位，详细情况见附件 1。

境外网络安全攻击 IP 地址中，归属于荷兰的 IP 地址（193.142.*.*）以 32520351 次攻击高居首位，美国有多个 IP 地址对黑龙江省关键信息基础设施开展网络安全攻击，单个 IP 地址的攻击次数少于上述荷兰 IP 地址，但攻击总次数则相对较高。详细情况见附件 2。

三、分析总结

综合分析亚冬会赛事信息系统和黑龙江省关键信息基础设施遭受境外攻击的情况，来自美国、荷兰等国家和地区的攻击较为密集。而且，值得注意的是，2025 年 1 月，中国国家互联网应急中心公开披露的关于美国情报机构针对我国大型科

科技企业机构的网络攻击事件调查报告¹中明确指出，美国频繁使用位于荷兰、德国等欧洲国家云主机作为跳板机或发起攻击的傀儡主机。对此，网络安全保障团队对攻击来源进行详细分析回溯，综合网络攻击源头的手法、工具、时间、语言等行为特征，高度怀疑此次涉亚冬会期间相关赛事信息系统和黑龙江省关键信息基础设施遭到的网络攻击具有美国政府支持的背景。

相关情况表明，在我国承办国际大型体育赛事期间，境外势力不遗余力地试图通过网络攻击手段破坏、干扰赛事正常进行，甚至妄图通过网络攻击关键信息基础设施制造混乱和窃取敏感情报。我们对这种针对重大国际民间交流活动的恶意网络攻击表示强烈谴责，并将恶意攻击细节提交公安机关。

国家计算机病毒应急处理中心
计算机病毒防治技术国家工程实验室
2025年4月3日

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

附件 1

排名前十位的境外攻击源分布情况

排名	IP 地址归属地	网络攻击次数
1	荷兰	37983182
2	美国	11798655
3	泰国	723451
4	澳大利亚	382540
5	英国	328726
6	德国	233509
7	立陶宛	189071
8	加拿大	168270
9	日本	97572
10	新加坡	63390

附件 2

排名前十位的境外攻击源 IP 地址具体情况

排名	IP 地址	IP 归属地	网络攻击次数
1	193.142.*.*	荷兰	32520351
2	204.76.*.*	美国	952981
3	204.76.*.*	美国	391062
4	83.164.*.*	奥地利	287506
5	98.197.*.*	美国	261124
6	98.197.*.*	美国	253287
7	98.197.*.*	美国	250986
8	98.197.*.*	美国	250973
9	98.197.*.*	美国	250551
10	98.197.*.*	美国	247645