2025年4月16日 星期三 齐鲁晚报

哈尔滨市公安局锁定境外网络攻击亚冬会犯罪嫌疑人

公开通缉3名美国国家安全局特工

记者15日从哈尔滨市公安局了解到，2025年哈尔滨第九届亚冬会期间，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。经查，美国国家安全局特定入侵行动办公室（简称“TAO”）三名特工参与实施了上述网络攻击活动。

为依法严厉打击境外势力对我国网攻窃密犯罪，切实维护国家网络空间安全和人民生命财产安全，哈尔滨市公安局决定对上述3名犯罪嫌疑人进行悬赏通缉。发现有关人员线索可立即向公安机关举报。

追踪溯源 锁定网络攻击幕后黑手

本月初，“2025年哈尔滨第九届亚冬会”遭受境外网络攻击事件经媒体报道后，引发广泛关注。国家计算机病毒应急处理中心和亚冬会赛事网络安全保障团队，及时向哈尔滨市公安局提交了亚冬会遭受网络攻击的全部数据。哈尔滨市公安局立即组织技术专家组成技术团队开展网络攻击溯源调查。在相关国家支持下，经技术团队持续攻坚，成功追查到美国国家安全局（NSA）的3名特工和两所美国高校，参与实施了针对亚冬会的网络攻击活动。现在，警方已掌握相关网络攻击的确凿证据，并决定对3名美国国家安全局特工进行悬赏通缉。

那么，这3名美国特工到底是谁？他们究竟做了什么呢？

4月3日，国家计算机病毒应急处理中心发布了一份报告，其中披露了2组数字，27万次和5000万次，这两组数字分别对应的是：哈尔滨亚冬会的赛事信息系统和黑龙江省内关键信息基础设施遭到境外网络攻击的次数，这里所说的境外攻击者，实际上就是美国及其盟友国家。

我国网络安全技术团队通过对攻击数据进行追踪溯源，在相关国家的支持下，最终锁定了此次攻击事件的幕后黑手——美国国家安全局（NSA）的3名特工，他们分别是：凯瑟琳·威尔逊（Katheryn A. Wilson）、罗伯特·思内尔（Robert J. Snelling）、斯蒂芬·约翰逊（Stephen W. Johnson）。通过进一步调查发现，这3名特工的累累前科被陆续挖出，他们曾多次对我国关键信息基础设施实施网络攻击，还参与了对华为公司等企业的网络攻击活动。

360集团创始人周鸿祎介绍，“早在几年前我们就多次发现，美国对西北工业大学和我国一系列关于科研军工关键基础设施的攻击之后，我们也大概用了10年时间建立了他的攻击手法，整个战术知识库。”“这次溯源到三个个人特工，这是重大突破”。

在确保赛事安全进行的同时，国家计算机病毒应急处理中心和亚冬会赛事网络安全保障团队，第一时间向哈尔滨警方提交了相关网络攻击的全部数据。哈尔滨市公安局高度重视此次网络攻击事件，立即组织技术专家组成技术团队开展网络攻击溯源调查。

奇安信科技集团总裁吴云坤介绍，针对亚冬会网络攻击高度定向，这些关键业务系统一旦出问题，无论是数据被偷走，或者被摧毁，对于整个赛事来说都有重大影响。“我们从IP地址上能看出，（攻击者）大多来自于像美国以及相应盟友的组织，所以这也代表国际上最高的网络攻击水平。”

据网络安全技术团队介绍，在此次追踪溯源的过程中还发现，美国在实施网络攻击中还使用了人工智能技术。周鸿祎介绍，“有些代码明显是人工智能书写的攻击代码，也就是实现了在攻击过程中可以自动快速地编写一个动态的代码来实施攻击的行为”。

美两所高校参与操作系统后门疑被激活

经技术团队层层溯源，此次针对亚冬会开展网络攻击是由美国国家安全局（NSA）精心组织实施的一次网络攻击行动，实施此次网络攻击行动的组织是美国国家安全局信息情报部（代号S）数据侦察局（代号S3）下属特定入侵行动办公室（Office of Tailored Access Operation，简称“TAO”，代号S32）。

调查发现，美国国家安全局（NSA）赛前攻击行为主要集中在亚冬会注册系统、抵离管理系统、竞赛报名系统等重要信息系统，这些系统用于赛前开展相关工作，保存了大量赛事相关人员身份敏感信息，美国国家安全局（NSA）意图利用网络攻击窃取参赛运动员的个人隐私数据。从2月3日第一场冰球比赛开始，美国国家安全局（NSA）网络攻击达到高峰，此时攻击重点方向为赛事信息发布系统（包括API接口）、抵离管理系统等，此类系统为赛事过程保障的重要信息系统，美国国家安全局（NSA）妄图破坏系统，扰乱亚冬会赛事的正常运行。

我国网络安全技术团队调查发现，该3名特工曾多次对我国关键信息基础设施实施网络攻击，并参与对华为公司等企业的网络攻击活动。技术团队同时发现，具有美国国家安全局（NSA）背景的美国加利福尼亚大学、弗吉尼亚理工大学也参与了本次网络攻击。

那么，美国国家安全局主导的这次网络攻击都实施了哪些手段？我们都是采取哪些措施进行应对的呢？

据公开信息：加利福尼亚大学自2015年起就被美国国家安全局和国土安全部指定为网络防御教育领域的学术卓越中心；而弗吉尼亚理工大学是美国6所高级军事院校之一，曾在2021年接受美国国家安全局资助，用于加强网络攻防的队伍建设。

杭州安恒信息技术股份有限公司董事长范渊介绍，通过溯源分析，我方发现美国多所高校参与了对亚冬会重要赛事系统的攻击。其中弗吉尼亚理工大学是美国知名的军事学校，该学校曾在不同时期接受了美国国家安全局、联邦调查局、国土安全部等情治部门的资助，用于加强网络攻防队伍和网络攻防靶场的建设，同样也是美国国家安全局认定的“网络安全作战研究中心”。“这种将高等教育资源武器化的行径，严重破坏了国际学术共同体的信任基石。”

经过技术团队的层层溯源发现，此次针对亚冬会开展的网络攻击，是由美国国家安全局精心组织实施的，具体实施部门为下属的特定入侵行动办公室。调查发现，特定入侵行动办公室为掩护其攻击来源和保护网络武器安全，利用所属的多家掩护机构购买了一批不同国家的IP地址，并匿名租用了一大批位于欧洲、亚洲等国家和地区的网络服务器。

国家计算机病毒应急处理中心高级工程师杜振华介绍，遭遇这种比较大规模的网络攻击，从攻击过程和方式上，主要体现在攻击者首先进行了大规模的网络设备资产探测，“意图是获取这些位于网络边缘的服务器或者网络设备的访问权限，随后试图建立立足点，再通过这些立足点逐步地向内网渗透，去投送更多的网络武器，实施内网的渗透，以及建立一种长期的潜伏的效果”。

据网络安全专家介绍，美国国家安全局此次开展的网络渗透攻击活动，涵盖数百类已知和未知的攻击手法，攻击方式超前，包括未知漏洞盲打、文件读取漏洞、备份文件以及敏感文件及路径探测攻击等，攻击目标、攻击意图非常明显。

安天集团创始人、董事长肖新光介绍，在这个过程中，我方感知拦截了来自境外的网络安全攻击，并进行深度分析处置，发现了相关关键威胁的线索和痕迹。“在为期493天整个的运行过程中，我们前置进行安全检查评估的支撑工作，前置处理了大量的威胁隐患，并且在最终进行了15天7×24小时23个点位的全面值守。”

另外，我国网络安全技术团队还发现，亚冬会期间美国国家安全局向黑龙江省内多个基于微软Windows操作系统的特定设备发送未知加密字节，疑为唤醒、激活微软Windows操作系统提前预留的特定后门。

哈尔滨市公安局决定，对上述3名犯罪嫌疑人进行悬赏通缉。发现有关人员线索可立即向公安机关举报，公安机关将对举报人身份信息严格保密。凡向公安机关提供有效线索的举报人，以及配合公安机关抓获有关犯罪嫌疑人的有功人员，公安机关将给予一定金额的奖励。

据新华社、央视

相关链接

外交部：

中方将继续采取一切必要措施保护自身网络安全

外交部发言人林剑15日表示，中方将继续采取一切必要措施保护自身的网络安全。

当日例行记者会上，有记者问：今天哈尔滨市公安局发布通告，悬赏通缉参与在第九届亚冬会期间对赛事信息系统和黑龙江省关键信息基础设施开展网络攻击的美国国家安全局有关人员。中方对此有何评论？

林剑表示，中方注意到有关报道。此前，中方已经多次阐述立场。在第九届亚冬会期间，美国政府针对赛事信息系统和黑龙江省内关键信息基础设施开展网络攻击，对中国关键信息基础设施、国防、金融、社会、生产以及公民个人信息安全造成严重危害，性质十分恶劣。中方谴责美国政府的上述恶意网络行为。

“中方已通过各种方式就美网络攻击中国关键基础设施向美方表明关切。”林剑说，中方敦促美方在网络安全问题上采取负责任的态度，停止对中方实施网络攻击，停止对中方无端抹黑和攻击。 **据新华社**

编辑：蓝峰 美编：马秀霞 组版：刘淼

报料电话：13869196706 欢迎下载齐鲁壹点 600多位在线记者等你报料

报纸发行：（0531）85196329 85196361 报纸广告：（0531）85196150 85196192 文字差错投诉：（0531）85193436 发行投诉：4006598116 （0531）85196527 邮政投递投诉：11185 全省统一零售价：1.5元

邮发：23-55 广告许可证：鲁工商广字01081号 地址：济南泺源大街2号 大众传媒大厦 邮编：250014 大众华泰印务公司(大众日报印刷厂印刷(济南市长清区玉皇山路1678号)