操弄网络攻击溯源 栽赃陷害中国
——揭开“伏特台风”真相

2024年2月1日，美国国会众议院“中国问题特别委员会”举行了“中国对美国国土和国家安全的网络威胁”听证会。会议围绕2023年5月被美国微软公司披露的名为“伏特台风”（Volt Typhoon）且所谓“具有中国政府支持背景的黑客组织”展开讨论，称其对美国关键基础设施发动了网络攻击并试图进一步实施破坏，给美国国家安全造成严重威胁。

“伏特台风”是何方神圣？其与中国政府的关联证据何在？既然去年5月就已经披露了攻击活动，美国政客为何时隔8个月旧事重提，再次向中国发难？

何为“伏特台风”？

2023年5月24日，“五眼联盟”国家（美国、英国、加拿大、澳大利亚、新西兰）的网络安全主管部门联合发布了名为《中华人民共和国国家支持背景的黑客正在使用逃避检测技术》的预警通报。预警通报称名为“伏特台风”的黑客组织针对美国关键基础设施单位实施了网络间谍活动。

该预警通报直接引用了微软公司于同日发布的《“伏特台风”组织利用逃避检测技术针对美国关键基础设施发动攻击》的技术分析报告和溯源分析结果。微软公司技术分析报告中将攻击者按照微软公司的内部规则命名为“伏特台风”，并直接指出该组织是所谓“总部位于中国且由国家政府支持的网络攻击行为主体”。

虽然“五眼联盟”的预警通报和微软公司的技术报告详细介绍了攻击者的技战术特征和感染指标等，但没有给出具体的溯源分析过程，而是直接给“伏特台风”打上了“具有中国政府支持背景的黑客组织”标签。

该预警通报一经发布就被路透社、华尔街日报、纽约时报等新闻媒体大量转载，纽约时报还报道称美国情报机构在2023年2月发现关岛和美国部分地区的电信网络遭到入侵，并将上述攻击与相关预警通报联系起来。

不难看出，关于“伏特台风”组织以及该组织的归属，美国政府、网络安全企业和新闻媒体的最主要参考依据就是微软公司的技术分析报告和“五眼联盟”发布的联合预警通报。

“伏特台风”真的具有国家支持背景吗？

一直以来，网络攻击活动的归因分析都是国际性难题。“伏特台风”这一名称和归因都源自美国微软公司的技术分析报告和“五眼联盟”发布的联合预警通报，但微软公司并没有给出详细的归因分析过程和根据，且报告中也提及，黑客使用逃避检测技术为取证和溯源工作带来较大困难。

中国国家计算机病毒应急处理中心和计算机病毒防治技术国家工程实验室联合360数字安全集团通过对报告给出的相关攻击活动技术特征进行溯源分析，发现能够被查找到的13个恶意程序样本关联多个IP地址。这些IP地址与很多的网络攻击事件相关，并且也存在多个IP地址与同一攻击事件或网络安全风险存在关联的现象，其中与13个恶意程序样本关联程度最高的有5个IP地址。

而与这5个IP地址都有关联的网络攻击事件报告是美国威胁盟公司于2023年4月11日发布的《关于“暗黑力量”勒索病毒团伙研究报告》。报告显示，“暗黑力量”首次被发现攻击活动时间为2023年1月，仅2023年3月全球范围内就至少有10个机构遭到该组织攻击并被勒索。受害机构所在国家包括阿尔及利亚、埃及、捷克、土耳其、以色列、秘鲁、法国、美国等。

另外，通过对美国流明科技公司2023年12月发布报告中包含的恶意程序样本和IP地址等技术特征进行检索，并未找到其与微软公司和“五眼联盟”预警通报中所述技术特征之间的关联关系。

技术团队判定，来自“伏特台风”的恶意程序样本并未表现出明确的国家背景黑客组织行为特征，而是与“暗黑力量”勒索病毒等网络犯罪团伙的关联程度明显。在此情况下，微软公司及“五眼联盟”国家仅凭受害单位和攻击者的攻击技战术这些模糊的归因因素就将“伏特台风”扣上所谓“中国政府黑客”的帽子未免过于牵强。

“伏特台风”的真相

2024年1月31日对于美国国会、美国政府网络安全主管部门和美国网络安全企业来说是一个重要的时间节点。在同一天，美国国会、美国司法部、美国国土安全部共同针对“伏特台风”打出了一套“组合拳”。

首先，参加听证会的美国国会议员以及美国国家安全局、美国网络安全与基础设施安全局、美国联邦调查局和美国国家网络总监办公室的一把手们大肆鼓吹“中国威胁论”，要求国会在网络安全方面进一步加大人、财、物投入。其次，2024年美国总统大选，共和、民主两党自然都不想在中国问题上“丢选票”，通过公开“讨伐”中国，国会议员们还可以提高自身曝光率，收获不错的政治资本。

美国网络安全企业当然希望美国联邦政府的钱包越鼓越好，而且“中国威胁论”也成为这些企业开拓欧美市场最好的营销广告。最终，在2024年3月11日，拜登政府公布的2025财年预算申请文件中，联邦政府在民事行政部门和机构的网络安全预算达到了创纪录的130亿美元，较2024财年又提高了10%。

就在微软公司发布报告的前两个月，也就是2023年3月24日，微软公司获得了美国国防部联合作战云项目的第一批任务订单。在美国流明科技公司发布有关KV僵尸网络与“伏特台风”存在关联的分析报告的前一个月，2023年11月7日，美国流明科技公司刚刚赢得了美国国防信息系统局价值1.1亿美元的五年期合同订单。

美国政客、高官和企业家因“伏特台风”虚假叙事赚得盆满钵满，而且也达到在国际社会抹黑中国形象、离间中国与他国关系、遏制中国经济发展的目的。

美国政府搞小圈子、小院高墙，甚至操弄微软等公司开展虚假叙事，把网络攻击溯源当成政治游戏、当成打压中国的工具、当成攫取资本为自身谋利的抓手，彻底暴露了美“歇斯底里”和“无底线”的对华政策，以及美国政客、高官和企业家勾连腐败真相，这样只会破坏国际公共网络空间的正常秩序，破坏中美关系，影响美国政府在全球的声誉。

近年来，中国公安机关侦破西北工业大学、武汉市地震监测中心等多个机构被美国家安全局、中央情报局网络攻击案件表明，美国才是真正的“黑客帝国”“窃密帝国”。 新华社北京4月15日电