揭开『伏特台风』真相——
美操弄网络攻击溯源 栽赃陷害中国

据新华社电 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,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”。

然而,无论是预警通报还是微软公司的技术报告,都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。

它有国家背景吗?

一直以来,网络攻击活动的归因分析都是国际性难题。对于“伏特台风”,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。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,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,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,大家一起鼓吹“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,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,“中国威胁论”自然是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%。

而微软公司在报告发布的前两个月,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,流明科技公司得到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。

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”。

国家安全部:

核心岗位涉密人员及高校师生成境外间谍情报机关重点目标

近日,国家安全部官方微信公众号推出4·15全民国家安全教育日重磅专题《创新引领·国安砺剑》,总结回顾总体国家安全观提出十年来,国家安全机关破获的十个重大间谍案件,起底了境外间谍情报机关渗透、窃密、策反的各式卑劣手法,同时展现了国安干警与人民群众携手捍卫国家安全的重要时刻。

美国“功勋”间谍出镜忏悔

专题公布的“十大反间谍案例”中,就包括梁成运案。在今年3月的全国两会期间,最高人民法院院长张军在作最高人民法院工作报告时提到,“依法惩处从事间谍活动的梁成运等,形成有力震慑”。

梁成运1945年出生于中国香港,现年79岁。1983年,梁成运赴美国经营餐厅,随后被美国间谍情报机关选中合作,1989年成为美国间谍情报机关线人。

美国间谍情报机关为梁成运虚构了丰富的履历,包括他在英国就读大学、在联合国担任官员、去越南参战等履历。为了扩大梁成运在中国的知名度,美方指挥其赴中国开展慈善捐款,设法将其打造为“爱国慈善家”。梁成运做美国间谍长达30多年,为美国间谍情报机关搜集了大量涉华情报,还被美方授予“功勋奖牌”。

2021年4月,梁成运被抓获归案。2023年5月,梁成运因犯间谍罪被判处无期徒刑,剥夺政治权利终身。“我很后悔,我想告诉所有的华人、中国人,他们(美方)的甜言蜜语是假的。”专题片中,一头白发的梁成运出镜忏悔。

国家安全部表示,近年来,随着我国综合国力不断提升,境外个别国家高度关注,一些境外间谍情报机关人员潜入我境内,想方设法打探情报、企图窃取我国家秘密。2018年12月,国家安全机关侦破康明凯、迈克尔为境外刺探、非法提供国家秘密、情报案。此外,我党政军机关、军工企业、科研院所等核心岗位涉密人员及高校师生是境外间谍情报机关开展情报搜集、渗透窃密的重点目标,对我国家安全构成严重威胁。

快艇驾驶员举报可疑人员偷拍军舰

国家安全部表示,近年来,越来越多人民群众及时通过各种方式,积极反映危害国家安全的可疑情况,为国家安全机关依法发现、防范、制止和惩治各类危害国家安全活动提供了有力支持。

2019年6月,广东某港口快艇驾驶员小马向国家安全机关举报,一外来“游客”乘其快艇,要求去某军港附近观光,趁机偷拍军舰,还制作简易示意图。经查,“游客”冉某是一名贪图小利的无知青年,被境外间谍情报机关利用。最终,冉某被判处有期徒刑5年,小马受到奖励。

■来源:国家安全部官方微信公众号