操弄网络攻击溯源 栽赃陷害中国

——揭开“伏特台风”真相

新华社记者

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)

以色列会如何报复『伊朗的报复』

新华社记者 吕迎旭 张天朗

以色列战时内阁14日召开会议研究如何反击伊朗13日夜对以色列的袭击,但没有宣布最终决定。以色列战时内阁成员甘茨同日在声明中说,以色列将“以适合我们的方式、在合适的时间,让伊朗付出代价”。

分析人士认为,伊朗此次袭击以色列本土,有着与包括美国在内的多方提前“通过气”的痕迹。由于美国不愿卷入冲突等因素,以色列可能会推迟对伊朗的反击,但也很难“忍气吞声”,或采取有限报复措施。

袭击或“通过气”

以色列公共广播公司14日晚间报道,虽然内阁成员就反击伊朗袭击达成一致,但在以色列总理内塔尼亚胡与美国总统拜登14日通话后,反击行动“在最后一刻被取消”。

有分析认为,伊朗因该国驻叙利亚使馆遇袭而对以色列展开报复,但美国在袭击发生前发出预警,伊朗继而如预警那样发动袭击,显然提前“通过气”。

以色列媒体14日援引以官员的话报道,伊朗对以发动袭击前“已经告知以方”。路透社14日援引土耳其外交消息人士的话报道,袭击发生前的几天里,伊朗、土耳其和美国进行了沟通,美国“通过我们向伊朗传达这样的信息:反应必须在一定限度内”。

以色列军方发言人14日说,超过300个无人机和导弹射向以色列,其中超过99%被拦截。伊朗发射了170架无人机、超过30枚巡航导弹和超过120枚弹道导弹。其中,数枚弹道导弹抵达以色列领土,对一处空军基地造成轻微破坏。

耶路撒冷希伯来大学国际关系专家约纳坦·弗里曼对新华社记者说,伊朗尽量减少以方伤亡,以免将冲突扩大。

专家指出,此次伊朗对以色列报复袭击虽然阵势很大,但“相对克制”。伊朗军事专家阿里·阿卜迪撰文指出,伊朗仅仅使用了其拥有的二流和三流武器。

伊朗政治研究员萨拉赫丁·赫迪韦说,伊朗有意避开以色列大城市目标,主要针对的是位于内盖夫沙漠以及以色列占领的叙利亚戈兰高地这样相对偏远地区的军事目标。这种有限度的打击旨在恢复伊朗的威慑力并防止过度激怒以色列。

反击或被推迟

分析人士认为,从目前情况看,以色列推迟反击伊朗的可能性很大。

首先,以色列的最大靠山美国反对反击伊朗。拜登在14日与内塔尼亚胡的通话中表示,美国将反对以色列对伊朗的任何反击。不少分析指出,美国总统选举临近,拜登政府正努力防止加沙以外的中东地区陷入冲突。西北大学伊朗研究中心主任李福泉对新华社记者说,美国根本不想看到以色列直接打击伊朗,美伊都希望控制冲突规模,都不愿被以色列“拉下水”成为直接冲突方。

其次,促成组建反伊朗联盟可能对以色列更有吸引力。伊朗伊斯兰革命卫队前指挥官侯赛因·穆加达姆接受卡塔尔半岛电视台采访时指出,以色列现阶段看到了一个机会,即组建一个由美国领导的国际联盟来对抗伊朗及其核计划,以色列过去几年一直未能说服美国组建这一联盟。他说,以色列有可能认为这比军事回应更可行。

第三,以色列应对伊朗此次袭击相对成功,损失较小,可以给民众以交代。以《新消息报》14日在报道中直言,以色列因这一原因取消了对伊朗的反击。与此同时,美国、英国、约旦等多国参与拦截行动,对以色列来说也是一个外交胜利。

第四,以色列国内有声音认为,应优先考虑南线加沙和北线与黎巴嫩真主党的战事,特别是从加沙带回被扣押的以色列人。

在以上因素中,美国的反对最为关键。以色列贝京—萨达特战略研究中心高级研究员埃亚勒·平科对新华社记者说,以色列一旦直接攻击伊朗本土,将引发严重后果。美国出手帮助以色列拦截伊朗导弹,就是要削弱以色列猛烈反击伊朗的动机。

不会“忍气吞声”

多年来,以色列和伊朗多以非直接对抗形式在中东地区博弈,这被称为“影子战争”。而此次伊朗袭击以色列是两国首次直接军事对抗。对此,弗里曼认为,这是一个新的态势,今后伊朗与以色列的博弈手段可能会包括直接从领土打击。

但也有观点认为,以伊直接对抗只是意外情况,双方博弈还会回归到之前模式。伊朗政治分析人士阿迈德·舒克里说,伊朗此次袭击似乎并不代表此前两国之间“影子战争”的结束,反而可能导致两国以更加隐蔽和间接的方式继续对抗。

不过无论如何,以色列恐怕很难对伊朗的袭击“忍气吞声”。有分析指出,伊朗此次袭击“伤害性不大、侮辱性极强”,这对在中东地区有着军事实力优越感的以色列而言难以接受。

以色列国家安全研究所高级研究员约埃尔·古赞斯基对新华社记者说,以色列虽然短期内可能不会攻击伊朗,但不可能在中东地区示弱。弗里曼认为,以色列可能会通过其他方式继续增加对伊朗的威慑力,比如继续打击伊朗在叙利亚、黎巴嫩等地的机构和人员。(参与记者:霍晶)

(新华社耶路撒冷4月15日电)

4月15日,澳大利亚悉尼维多利亚女王大厦降半旗。

当日,澳大利亚各地降半旗,悼念13日悉尼商场持刀袭击事件中的遇难者。

新华社记者 马平 摄

悉尼再次发生持刀袭击事件

新华社悉尼4月15日电(记者李晓渝 王琪)澳大利亚警方15日说,悉尼西南部韦克利地区一座教堂当天发生持刀袭击事件,造成多人受伤,凶手已被警方逮捕。

澳大利亚新南威尔士州警方在警情通报中说,警方于当地时间19点10分许接到报案并赶往现场。目前已经逮捕一名男性。受伤者已接受救治,均无生命危险。

警方表示正在开展大规模应对行动,并敦促民众远离事发地区。

悉尼东南部一家大型购物中心13日发生一起持刀袭击事件,已致6人死亡,另有至少12人受伤。凶手被警方当场击毙。

缅甸中部一城镇遭袭4死12伤

新华社仰光4月15日电(记者张东强 黎广滔)缅甸国家管理委员会15日发布消息说,恐怖分子14日晚炮击曼德勒省彬乌伦镇,造成4人死亡、12人受伤。

消息说,恐怖分子从彬乌伦镇西边向镇区发射了11枚火箭炮,炮弹落入医院、寺庙、酒店等建筑物,造成包括2名僧侣在内的4人死亡,另有12人受伤,目前伤者均已得到救治。安全部队已经加强安保,并对实施破坏的恐怖分子展开抓捕行动。

另据缅甸国家管理委员会14日发布的消息,恐怖分子在曼德勒省千埃达赞镇区市政泼水节庆祝台阴近制造爆炸事件,造成12人受伤。

近几日正值缅甸传统泼水节。据缅甸媒体报道,恐怖分子在泼水节期间使用无人机、火箭弹和自制炸弹向城镇和村庄发动袭击,制造恐慌。

国网长岭县供电公司:

开展“双报到”志愿服务活动

为推进“双报到、双服务”活动实效,国网长岭县供电公司于近日,组织6名共产党员服务队队员到长兴路社区报到,开展志愿服务活动。该公司积极开展“双报到”活动,指定一名联络员定期沟通街道社区。制定计划,每季度与街道社区党组织开展1次共建活动,帮助社区协调解决难点问题。该公司积极发挥自身行业优势,组织共产党员服务队定期对社区居民用电安全隐患进行排查治理工作,义务为困难群众家庭更换进户线和室内开关,为社区广大居民消除用电安全隐患。同时,加入社区志愿者队伍,帮助社区开展环境整治工作。通过开展“双报到”活动,该公司号召全体党员进一步发挥先锋模范作用,着力解决好群众身边的操心事、烦心事,为建设美好和谐社区贡献一份力量。(候宪洋)

为企纾困 倾情调解

本报讯(黄国丽)近日,长春经开法院成功调解一起买卖合同纠纷案。在承办法官的多番协调下,既保障了原告企业权益,也让企业从“两难”变为“双赢”。

原告某建材店向被告某劳务公司追索货款未果,诉至法院。送达过程中,被告始终态度消极。考虑到通话过程中被告反复强调不是故意违约,开庭当日,法官再次给被告发送短信,告知其下午开庭等信息,被告仍未到庭。缺席审理后,当天晚上法官接到了被告的电话,他表示自己一直在外地要账,企业陷入财务困境,希望法官能从中调解,让企业缓口气。

法官了解情况后,第一时间向原告转达被告公司希望化解矛盾的意思,法官劝解双方,各让一步不仅能维护合作伙伴关系,而且调解结案更能保障公正与效率。承办法官多次组织双方对账,帮助当事人厘清具体情况,最终双方确定了欠款金额并达成分期还款调解协议,缓解了被告企业经济压力,原告的合法诉求也得到了保障。