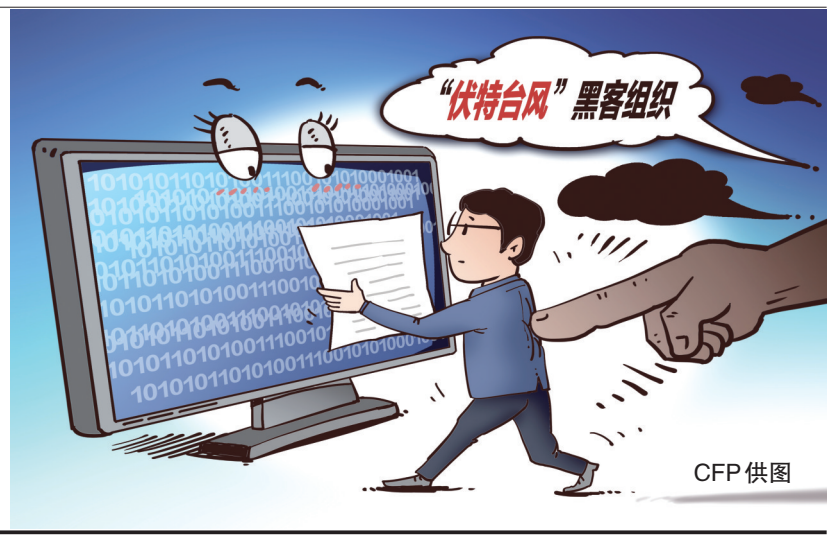
操弄网络攻击溯源 栽赃陷害中国

——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。



CFP供图

“五眼联盟”国家单方面定性

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。

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。

具有国家支持背景理由牵强

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。

虚假叙事意在抹黑中国形象

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,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。

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。

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”。**据新华视点**

爱养“异宠” 可能危害国家安全

近些年,一些追求所谓新潮和猎奇的宠物爱好者,通过非法途径和渠道从国外进口“异宠”。这些“异宠”,可能自身带有剧毒,也可能携带疫病,对我国的生态环境造成不可预估的破坏。

走私“异宠”入境伪装隐蔽

今年2月,在云南河口口岸,一名腰腹臃肿、步态异常的入境旅客引起现场海关关员注意。检查发现,该旅客腰部用胶带缠裹着大量塑料指型管,每个指型管均单独存放着一只活体蚂蚁,共163只。经送检鉴定,该批蚂蚁为野蛮收获蚁。

自2023年以来,我国多地海关截获秘密入境的有害生物。为保护我国生态安全和生物多样性,海关总署部署为期三年的严防外来物种入侵专项行动,公安部开展了“昆仑2023”专项行动。2023年8月,海口海关缉私局联合海南省公安厅海岸警察总队、海南省公安厅森林公安局和深圳、广州、上海等多地海关缉私部门,开展了打击“异宠”走私集中收网行动,在8地14市抓获嫌疑人30名,打掉14个非法“异宠”繁育基地。

外来物种入侵有危害

生态系统是经过长期演化形成的,系统中的物种经过漫长的竞争、排斥、适应和互利互助,才形成了相互依赖又互相制约的密切关系。一个外来物种的到来,可能因新环境中没有制约它的生物,最终成为入侵者,改变或破坏当地的生态环境、生物多样性,还会对经济社会和人民群众生活带来负面影响。

湖南农业大学生物科学技术学院副院长杨华介绍,入侵物种的生命力强大,容易导致周边的其他物种消亡。比如薇甘菊在广东发现后,很快伶仃岛的其他物种基本找不到了。

外来物种入侵还会对人的健康造成影响,比如红火蚁直接咬人的手或是其他部位,可能导致溃疡,甚至过敏死亡。

擅自携带、寄递进境“异宠”会获罪

一些擅自携带、邮寄进境“异宠”的行为可能已碰触法律红线,需要承担相应的法律责任。2021年施行的《刑法修正案(十一)》新增“非法引进、释放、丢弃外来入侵物种罪”。

2022年,拱北海关关员在检查一位易姓男子驾驶的车辆时,从天窗和遮阳板夹缝处及扶手箱改装的暗格内发现2000多只活体龟类动物,却不能出具有效的检疫审批证明。

经拱北海关技术检测,涉案活体龟类动物中有2015只为巴西红耳龟,而巴西红耳龟已被列入《中国外来入侵物种名单》第三批名单内并被世界自然保护联盟列为100种最危险入侵物种之一。今年4月12日,广东珠海市人民检察院以涉嫌非法引进外来入侵物种罪对易某提起了公诉。该案是全国首例检察机关提起公诉的非法引进外来入侵物种案。

据央视新闻微信公众号