

操弄网络攻击溯源 栽赃陷害中国

——揭开“伏特台风”真相

新华社北京4月15日电 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“中国对美国国土和网络安全网络威胁”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“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。预警通报称何为“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“总部位于中国且由美国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、民主两党自然都不愿在中国问题上“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139亿美元,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、离间中国与外国关系、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”。

但从方案提出之初,现场安保就成为组织者面临的最大难题。而法国面临的潜在恐袭风险增加,也是组委会和法国政府不得不考虑的因素。

接下来的一段时间,巴黎奥运会的筹备工作进入最后冲刺阶段。巴黎奥运会火种将于4月16日在希腊古奥林匹亚采集。4月17日,巴黎奥运会将迎来倒计时100天。

第135届广交会开幕



4月15日,中外客商行走在第135届广交会展馆内。

当日,第135届中国进出口商品交易会在广州开幕。本届广交会展示先进制造成果,预计现场新品超100万件;境外采购商参会意愿加强。

本届广交会总展览面积155万平方米,展位总数约7.4万个,参展企业2.9万家;截至14日,有215个国家和地区的14.9万名境外采购商预注册,较上届增长17.4%。

本届广交会于4月15日至5月5日分三期举办线下展,主题依次是“先进制造”“品质家居”“美好生活”。

新华社记者 刘大伟 摄

就伊朗袭击以色列 安理会举行紧急会议

据新华社联合国4月14日电(记者 尚绪谦)联合国安理会14日就伊朗袭击以色列举行紧急会议,联合国秘书长古特雷斯在讲话中敦促各方保持最大限度的克制。

古特雷斯说,中东地区面临全面冲突的风险。现在是缓和降级、保持最大限度克制的时候了。《联合国宪章》禁止以武力侵害任何国家的领土完整或政治独立,同时外交馆舍与外交人员不可侵犯的国际法原则必须得到尊重。

古特雷斯敦促各方避免采取可能引发大规模军事冲突的任何行动。他说,国际社会有共同责任与有关各方积极接触,避免局势进一步升级,谋求在加沙地带立即实现人道主义停火,争取被扣押人员获释,保证人道救援顺利进行。国际社会有共同责任停止约旦河西岸的暴力,缓和以色列与黎巴嫩边境紧张局势,重新确立红海的航行安全。

古特雷斯说,中东地区和全球的和平与安全时时受到破坏,中东地区 and 世界难以承受更多的战争。

声明作废

- ▲舟山市定海弘金机械厂遗失公章一枚。
- ▲舟源清16遗失国内航行海船安全与环保证书,船检登记号:2011V2101182,船舶识别号:CN20105221808。
- ▲舟山市瑞航海运有限公司所属船舶鑫瑞26遗失国内航行海船安全与环保证书一本,船检登记号:2004T3100283。

舟山市地质灾害隐患点及防治责任人公告

根据《地质灾害防治条例》(国务院令第394号)和《浙江省地质灾害防治条例》,2024年3月舟山市自然资源和规划局对全市地质灾害隐患点进行了拉网式巡查和排查,经巡排查,全市新发现地质灾害隐患点7处。为充分有效地发挥地质灾害防治过程中的群测群防效能,最大限度地减少地质灾害带来的损失,保护人民群众的生命财产安全,现将舟山市地质灾害隐患点及防治责任人予以公告。各地要按照《2024年舟山市地质灾害防治方案》要求,及时开展各项防治工作,确保安全度汛。

序号	位 置	灾种	规模	受威胁户数	受威胁人数	受威胁财产(万元)	监测责任人		所属区域	乡(镇、街道)防灾责任人			县(区)防灾责任人		
							姓名	电话		姓名	单位职务	电话	姓名	单位职务	电话
1	定海区白泉镇梅山禅寺前侧道路滑坡地质灾害隐患点	滑坡	小型	0	行人	2	叶军杰	13705802025	白泉镇	陈 卓	副书记	13868245717	夏 泉	常务副区长	0580-2049571
2	普陀区桃花镇茅山村上稻蓬26号屋后边坡地质灾害隐患点	崩塌	小型	0	3	230	王涛涛	13867225162	桃花镇	刘 怡	镇长	13967206036	朱彦波	副区长	0580-3065039
3	岱山县东沙镇泥峙村黄沙湾 12-21 号屋后边坡地质灾害隐患点	崩塌	小型	2	3	196.75	毛明达	13868222607	东沙镇	张 鋈	镇长	15958095820	陈华清	常务副县长	0580-4406276
4	岱山县衢山镇田涂村舒心亭下道路边坡地质灾害隐患点	崩塌	小型	0	0	50	金科技	13758006724	衢山镇	沈飞腾	镇长	13575636495	陈华清	常务副县长	0580-4406276
5	岱山县衢山镇田涂村浦港路67号屋后边坡地质灾害隐患点	崩塌	小型	2	3	100	金科技	13758006724	衢山镇	沈飞腾	镇长	13575636495	陈华清	常务副县长	0580-4406276
6	岱山县衢山镇打水村康庄路南侧屋后边坡地质灾害隐患点	崩塌	小型	0	1	200	顾贤军	13967229342	衢山镇	沈飞腾	镇长	13575636495	陈华清	常务副县长	0580-4406276
7	嵊泗县嵊山镇箱子岙村箱西路5号屋后边坡地质灾害隐患点	崩塌	小型	0	行人	50	董思雨	18768051509	嵊山镇	张 超	镇长	13454060496	周国宏	副县长	0580-5598206

中国体育彩票开奖信息

第24042期体彩大乐透开奖号码:前区01 08 15 23 35 后区05 12
第24096期体彩排列3开奖号码:4 6 3
第24096期体彩排列5开奖号码:4 6 3 5 2
第24096期体彩20选5开奖号码:10 11 12 18 20

本信息如与公证开奖结果不符,以后者为准。咨询电话:0580-2861788 <http://www.zslottery.com>

中国福利彩票开奖公告

七乐彩 第2024042期 基本号: 09 12 16 20 21 23 26 特别号:27
6 + 1 第2024042期 基本号: 3 5 5 3 9 0 生肖码:猪
15选5 第2024096期 基本号: 07 08 11 12 13
3 D 第2024096期 开奖号码: 1 2 9

开奖信息如有差错,以省福彩中心公告为准。咨询电话:0580-2022721

超级大乐透 陪伴逐梦奋斗的你 相伴三十载 10亿大派奖周年庆活动来袭!

来之于民 用之于民
中国体育彩票已累计筹集公益金超8000亿元 我们都是公益事业参与者
严厉打击私彩 远离非法彩票



扫一扫了解更多“舟山体彩”信息

舟山福彩面向社会公开征召经营者, 有更多补助政策帮助你顺利经营!

(详情请关注“舟山福彩”微信公众号)



扫一扫关注