

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的网络安全威胁”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组织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”。

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。

“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协盟公司于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》。

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管理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%。

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、离间中国与它国关系、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”。

(据新华社电)

国际观察

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。

悉尼持刀袭击事件中 受伤中国留学生无生命危险

据新华社电 新华社记者15日从中国驻澳大利亚使馆和驻悉尼总领馆了解到,在13日悉尼持刀袭击事件中受伤的中国留学生已得到及时救治,无生命危险。

中国驻澳大利亚使馆发言人说,4月13日下午,悉尼一家购物中心发生持刀行凶事件,中国驻澳使馆和驻悉尼总领馆高度关注,第一时间向澳方了解核实并表达关切,对一名中国留学生不幸遇难、另一名中国留学生受重伤深感震惊和万

分悲痛。中国驻澳使馆和驻悉尼总领馆将继续同澳方保持密切沟通,全力为一名中方遇难者的家属,以及一名伤者及其家属提供协助。

记者15日向中国驻悉尼总领馆了解到,目前,总领馆已同事件中中方遇难者和伤者的家属取得联系,并于当日派工作人员陪同遇难者家属处理善后事宜,前往医院看望伤者。伤者已得到及时救治,无生命危险。总领馆将继续同有关部门保持密切联系,做好后续事宜。

黄金价格还能涨多久

据新华社电 黄金价格近期一路高歌,连创历史新高。截至4月12日的14个交易日中,美国黄金期货价格11个交易日收涨,一度站上每盎司2400美元。分析人士认为,近期美国通胀反弹、地缘政治等因素均支持金价上涨。不过,由于黄金已极度超买,近期金价或

回调整理,中长期来看金价仍有上涨空间。

分析机构认为,由于没有迹象显示全球主要央行购买黄金的速度将放缓,金价仍有上涨潜能。有机构甚至预测,2024年的“淘金热”才刚刚开始,热度或将持续2至3年,金价仍处于周期性上升通道中。

马克龙：巴黎奥运会开幕式存在“备选方案”

据新华社电 法国总统马克龙15日在接受法国媒体采访时谈到了即将于7月26日在塞纳河上举行的巴黎奥运会开幕式,他表示如果安全风险过高,可能会放弃在塞纳河上举办。

巴黎即将迎来奥运倒计时100天的重要时刻,马克龙在大皇

宫内接受了法国媒体RMC与BFM TV的联合采访。在谈到备受关注的这场在塞纳河上举行的奥运开幕式时,马克龙再次重申了对成功举办这场开幕式的信心,但同时也表示,鉴于可能存在的安全风险,备选计划也在研究当中。

新加坡总理李显龙5月交棒给黄循财

据新华社电 新加坡总理公署15日发表声明宣布,总理李显龙将于5月15日辞职。他将正式向总统建议,由副总理兼财政部长黄循财出任新总理。

声明说,新加坡人民行动党的议员一致支持黄循财担任新总

理。新总理将于5月15日晚8时在新加坡总统府宣誓就职。

黄循财,现年51岁,2011年首次当选议员,曾在新加坡国防、通讯及新闻、文化、国家发展、教育、财政等部门任职,曾任新加坡抗击新冠疫情工作组负责人。

维护未成年人合法权益 优化未成年人成长环境



中宣部宣教局 中国文明网