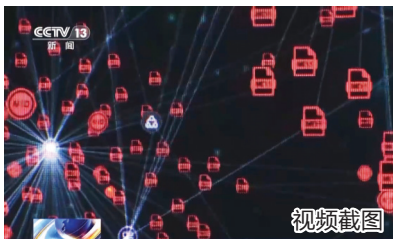
外交部：敦促美方立即停止对中国的网络攻击和污蔑抹黑

借口“伏特台风” 美栽赃陷害中国



昨天上午，中国国家计算机病毒应急处理中心发布了“伏特台风——美国情报机构针对美国国会和纳税人的合谋欺诈行动”报告，报告中揭露了美国情报机构利用毫无事实依据的，所谓“中国网络攻击威胁”的借口无底线抹黑中国，以此换取美国政府拨款的巨大丑闻。

昨日，外交部发言人林剑主持例行记者会回应相关问题时表示：众所周知，美国才是最大的网络攻击来源地，是网络空间安全的最大威胁。一段时间以来，美国一些人“贼喊捉贼”，把网络攻击溯源当成打压中国的工具，将网络安全问题政治化，严重侵害中方合法权益。中方敦促美方立即停止对中国的网络攻击，停止对中国的污蔑抹黑。

今年2月1日，美国众议院举行了一场所谓“中国网络攻击威胁”的听证会，该会议主要围绕2023年5月被美国微软公司披露的“伏特台风”黑客组织展开讨论，微软公司声称该黑客组织“具有中国政府支持背景”，并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。针对这一指控，中国的联合调查技术团队进行了溯源分析后发现，相关指控缺乏证据，纯属栽赃陷害，目的就是为了打压中国对外形象与发展。

何为“伏特台风”？

国家计算机病毒应急处理中心高级工程师杜振华介绍：“伏特台风组织的名称来自于微软公司，微软公司对所谓的具有国家支持背景的黑客组织，有一套自己的命名体系。其中台风这个别名，实际上就是微软公司所谓的具有中国国家支持背景的黑客组织的一个命名。”

据了解，2023年5月24日，微软公司发布《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，声称“伏特台风”黑客组织为“具有中国政府支持背景”，紧接着“五眼联盟”国家网络安全主管部门公开援引该报告，并进行大肆渲染。针对报告中的指控，中国国家计算机病毒应急处理中心第一时间联合360数字安全集团成立技术团队开展调查工作，并形成“伏特台风”溯源报告。

杜振华表示，微软公司在报告里面附带了很多的所谓感染指标，感染指标其实就是哈希值。这些哈希值我们可以想象成是一个恶意程序的编码、唯一的编号，通过对这些恶意程序的哈希值，在公开的平台上检索最后发现，有5个IP地址（关联样本）是最集中的。这5个IP地址也与很多的安全事件有关系，这些安全事件中就有一个（关于）叫Dark power，一个所谓的勒索病毒团伙一个分析报告有关系，这个分析报告是谁做？就是美国的ThreatMon，也叫威胁盟公司。

联合调查技术团队发现，2023年4月11日，在美国威胁盟公司发布的《关于“暗黑力量”勒索病毒团伙研究报告》中显示，上述恶意程序样本技术特征与一个名为“暗黑力量”的勒索病毒网络犯罪团伙关联程度密切，这个犯罪团伙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个以上的机构遭到该组织攻击并被勒索，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。

360数字安全集团网络安全专家边亮表示：“除了对IP地址的分析之外，我们对报告提到的恶意样本也进行了分析，该样本主要使用了无文件攻击，与传统的病毒木马不同，攻击载荷不需要写入磁盘，恶意代码在内存当中执行，重启和关机就会消失。样本的功能只是针对用户的文档进行加密、勒索索要赎金，所以我们认为这些样本和对应的IP地址都指向了勒索病毒犯罪团伙。”

联合调查技术团队经过溯源分析认为，微软公司和“五眼联盟”国家报告中提到的病毒程序并没有表现出明确的国家背景黑客组织行为特征，反而与勒索病毒网络犯罪团伙的关联程度更为明显。在这种情况下，微软公司和“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，就把“伏特台风”扣上所谓“中国政府支持背景黑客组织”的帽子，这样的做法是非常不严谨和不专业的，其背后必然有更深层次的原因。

美国扮成网络攻击“受害者” 对他国栽赃抹黑

据网络安全专家介绍，针对“伏特台风”组织的归因分析，美国的不同安全公司也有不同的观点，有的安全厂商认为它是一个僵尸网络，有的认为是APT（国家级黑客）组织，有的则认为是勒索病毒犯罪团伙。一直以来，网络攻击活动的归因分析都是国际性难题，但是美国政府却利用对他国网络攻击活动的归因，将自己塑造成被网络攻击的所谓“受害者”形象，在博取国际舆论支持的同时，将其作为政治筹码在国际争端中向他国施压，进而谋求超额利益。

据网络安全专家介绍，针对黑客组织的归因是一个非常复杂的过程，攻击者会通过各种手段隐藏自己的真实身份和地理位置，比如使用虚拟私人网络（VPN）、跳板机以及通过劫持受感染的计算机作为中继点来发起攻击，这些都使得追踪原始攻击源变得极其困难。

边亮表示：“另一个挑战是，攻击者可能会故意留下一些具有误导性的线索，他们可能会使用别国的语言、符号、时间戳作为伪装成其他黑客组织的特定行为模式，以误导调查人员，因此对APT（国家背景黑客）组织的归因，通常是在收集了大量数据之后，基于权衡数据的可能性，归因通常也只是能达到一定程度的信任水平，想要做到绝对的确定性是非常困难的。”

美国棱镜门事件相关报告提到，美国NSA（美国国家安全局）会入侵渗透国外资产，使用中间人劫持技术，窃取他国工具，实现干扰目的；美国CIA（美国中央情报局）报告提到，通过干扰嫁祸的方式，以避免外国敌对情报组织、执法、事件响应、逆向工程；“五眼联盟”中的加拿大通信局在安全架构设计中提到，通过相关欺骗技术，使用假旗行动制造动荡局面，改变对手感知，干扰嫁祸给其他国家；因此，对APT组织的归因通常是基于权衡证据的可能性，而不是绝对的黑白分明。

近年来，中国公安机关侦破西北工业大学、武汉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”。

杜振华说：“美国的NSA包括CIA都有过很多的网络武器泄露事件，导致现在的网络空间上出现了攻击能力不断增强的现状。这样的现状导致很多的网络犯罪团伙实际上具备的攻击能力是很强的。”

网络安全专家介绍，目前网络攻击基本以跨境犯罪为主，各国需要在国际刑警组织的框架下加强合作，共同分享网络犯罪的情报信息和协同治理，共同对抗网络安全威胁，而不是个别几个国家搞小圈子。

专访外交部网络事务协调员： “伏特台风”实为国际勒索软件组织

针对国家计算机病毒应急处理中心发布的报告，总台央视记者专访了外交部网络事务协调员王磊。王磊指出，这份报告揭露了一个只要无底线抹黑中国，就能换取美国政府拨款的巨大丑闻。

据溯源报告显示，2024年1月31日这个时间节点非常关键。按照美国相关法律，总统必须在每年2月第一个周一，也就是2024年2月5日前提交联邦政府下一财年预算申请。在2024年3月11日拜登政府公布的2025财年预算申请文件中，美国联邦政府的网络安全总预算和相关情报机构的网络安全预算都得到了显著增加。由此，报告认为，“伏特台风”就是美国情报机构和反华政客针对美国国会和纳税人的一次合谋欺诈。一方面通过操弄微软等网络安全企业捕风捉影，虚假叙事；另一方面利用手中的行政权力大肆渲染“中国网络攻击威胁”，欺骗美国国会不断增加网络安全预算。

王磊表示，美国的高官信誓旦旦地宣称，中国支持的黑客组织对关岛的关键基础设施进行了网络攻击。针对这一指控，报告揭露了一个重要的真相，得出了重要的结论。这个所谓“伏特台风”的真实面目是国际勒索软件组织。但是美方的网络安全机构和企业勾连腐败，对中国进行栽赃陷害，在获得部门和经济利益的同时，也为美国对华关系增添了非理性因素。

王磊强调，在中美关系中，网络安全一直是一个重要且特殊的议题，“全世界都很奇怪，全球最大的‘黑客帝国’美国为什么总是隔三差五地炒作‘中国黑客威胁论’。这份报告，就为我们解开问题的真相提供了重要依据和参考。更令人关注的是，在炒作‘伏特台风’期间，美方首次把网络安全与台海局势相联系。我们的立场十分清楚，我们反对利用网络安全问题干涉中国内政，对美方这种先制造议题，再借题发挥的真实意图，会保持警惕。在台湾问题上，打什么牌都是白费力气。”

王磊表示，保护关键基础设施是各国共同关切，维护网络空间的和平与稳定符合中美和全球各国的共同利益。“作为一个大国，希望美方能采取更严肃、更负责任的态度，也奉劝美方不要高估自己任意妄为单方面制定规则的‘实力’，更不应低估中方在平等的基础上维护中美网络关系的决心。”

据央视新闻频道

2024年4月16日 星期二
监制/续蓓 责编/王健 美编/张驰 责校/王永波
新报
新报微信平台