实施窃听窃密 蓄意嫁祸他国

揭秘美国政府机构实施的网络间谍和虚假信息行动

今年以来,中国国家计算机病毒应急处理中心等机构先后发布专题报告,全面揭露美国政府机构对全球电信和互联网用户实施无差别监听,并为背后相关利益集团攫取更大的政治利益和经济利益,虚构子虚乌有的中国网络攻击威胁,合谋欺诈美国国会议员和纳税人的事实。

近日,相关机构再次发布专题报告,进一步公开美国联邦政府、情报机构和"五眼联盟"国家针对中国和其他国家及全球互联网用户联合实施网络间谍窃听窃密活动,并通过误导溯源归因分析的隐身"工具包"实施"假旗"行动掩盖恶意网络攻击行为、嫁祸他国的铁证,彻底揭穿"伏特台风"这场由美国联邦政府自编自导自演的政治闹剧真相。

资料图片

网络空间的"变色龙"

此前,中国国家计算机病毒应急处理中心已经连续公开披露多款美国国家安全局(NSA)、中央情报局(CIA)开发的网络武器,详细分析了相关美国情报机构在对外网络攻击中所用的多款网络武器的功能,以及采用的高隐蔽性攻击技战术,但这些显然只是美国"黑客帝国"庞大网络武器库的"冰山一角"。

长期以来,美国在网络空间积极推行"防御前置"战略并实施"前出狩猎"战术行动,也就是在对手国家周边地区部署网络战部队,对这些国家的网上目标进行抵近侦察和网络渗透。为适应这种战术需要,美国情报机构专门研发用于掩盖自身恶意网络攻击行为、嫁祸他国并误导溯源归因分析的隐身"工具包",代号"大理石"(Marble)。该工具包是一个工具框架,可以与其他网络武器开发项目集成,辅助网络武器开发者对程序代码中各种可识别特征进行"混淆",有效"擦除"网络武器开发者的"指纹",使调查人员无法从技术角度追溯武器的真实来源。

该框架还有一个更加"无耻"的功能,就是可以随意插入中文、俄文、朝鲜文、波斯文、阿拉伯文等其他语种的字符串,这显然是为了误导调查人员,并栽赃陷害中国、俄罗斯、朝鲜、伊朗以及众多的阿拉伯国家。

"大理石"工具包框架充分暴露了美国情报机构在全世界开展的无差别、无底线网络间谍活动,并实施"假旗"(False Flag)行动,以误导调查人员和研究人员,实现栽赃"对手国家"的阴谋。

这种"假旗"行动并不仅限于代码特征层面,通过巧妙模仿网络犯罪团伙的攻击技战术,美国情报机构还可以虚构出各类完美的"口袋"组织。因此,美国网络战部队和情报机构的黑客就如同变色龙一般在网络空间中任意变换身份、变更形象,"代表"其他国家在全球实施网络攻击窃密活动,并将脏水泼向美国的非"盟友"国家。"伏特台风"行动就是一个典型的、精心设计的、符合美国资本集团利益的虚假信息行动。

网络空间的"窥探者"

据美国国家安全局的资料显示,美国依托其在互联网布局建设中先天掌握的技术优势和地理位置优势,牢牢把持全球最重要的大西洋海底光缆和太平洋海底光缆等互联网"咽喉要道",先后建立7个国家级的全流量监听站,与美国联邦调查局(FBI)和英国国家网络安全中心(NCSC)紧密合作,对光缆中传输的全量数据深度开展协议解析和数据窃取,实现对全球互联网用户的无差别监听。

这些互联网数据监听的受益者众多,除了美国联邦政府情报机构和军事机构外,还有大量美国联邦政府行政部门,包括白宫、内阁官员、美国驻外大使馆、美国贸易代表办公室、美国国会,以及美国国务院、农业部、司法部、财政部、能源部、商务部、国土安全部等。"伏特台风"计划的参与者不仅仅限于美国情报机构,而是为了服务所谓美国资本的共同利益,很多美国政府机构都在其中起到了推波助澜作用。

情报监听的输出结果必然是各种可读的信息和数据,因此把海底光缆中的传输流量实时转化、翻译成可阅读、可检索的情报信息是美国国家安全局的另一项重要工作。为解决这个问题,美国国家安全局实施了两个重点工程项目:一是"上游"(UpStream)项目,主要功能是将前述监听站拦截的海底光缆原始通信数据进行全量留存,形成规模庞大的数据"水库"。二是"棱镜"(Prism)项目,其主要功能一方面是将"上游"项目中的原始通信数据按照互联网应用进行分类,并对通信内容进行还原分析;另一方面,为有效解决"上游"项目中的加密数据破解和网络通信流量路径覆盖不全等突出问题,美国政府强制规定"棱镜"项目直接从美国各大互联网企业的服务器上获取用户数据。

从美国国家安全局的文件中可以看到,隶属于美国国家安全局的"特定入侵行动办公室"(TAO)在全球范围内发动无差别的网络秘密入侵行动,并植入了超过5万个间谍程序(Implants),受害目标主要集中在亚洲地区、东欧地区、非洲地区、中东地区和南美地区。从美国国家安全局的内部文件中可以清楚看到,中国境内的主要城市几乎都在其网络秘密入侵行动范围内,大量的互联网资产已经遭到入侵。上述间谍软件程序的命令控制中心很多都位于美国本土之外的军事基地。

事出反常必有妖

在第二份关于"伏特台风"调查报告发布后,虽然美国官方机构与其主流媒体仍然保持沉默,但一些前任和现任美国政府机构官员以及部分美国网络安全公司通过社交媒体平台、美国的网络安全行业媒体和独立新闻媒体表达了对我方调查报告的观点与看法,其中不乏一些负面声音,声称我方报告"歪曲""滥用"了美国相关公司的研究成果,这些美国公司也争先恐后地发声"撇清关系"。

"威胁盟"公司的改口行为特别耐人寻味。该公司在接受媒体采访时声称,由于其在后续研究中发现了前期涉"伏特台风"报告中提供的感染指标存在错误才修改了原报告,这种"敷衍"的解释更加令人怀疑。"威胁盟"这种异常举动,只能说明其对原报告的篡改过程是在强大外部压力下被动而匆忙完成的。最新报告中的证据充分表明,美国情报机构对中国、俄罗斯、伊朗和阿拉伯国家实施的网络间谍活动,以及针对美国国会和纳税人实施的虚假信息行动是铁一般的事实。

微软公司威胁情报战略总监德格里波在2024年度黑帽大会(BlackHat)期间表示所谓的"伏特台风"组织仍在活跃,且没有停止的迹象,却仍然没有给出任何能够说明该组织具有所谓"中国政府支持背景"的确凿证据。

多年来,美国联邦政府机构出于自身一己私利,不断将网络攻击溯源问题政治化,一些像微软和CrowdStrike这样的公司则为了迎合美国政客、政府机构和情报机构,出于提高自身商业利益考虑,在缺乏足够证据和严谨技术分析的情况下,热衷于用各种各样稀奇古怪且带有明显地缘政治色彩的名字对黑客组织进行命名。

中国一向反对政治操弄网络安全事件的技术调查,反对将网络攻击溯源归因问题政治化。而美国联邦政府机构则不断在幕后教唆纵容,在通过编造子虚乌有的网络攻击威胁骗取了大量国会预算后,野心越来越大,终有一天将会"搬起石头砸自己的脚"。克里斯托弗·雷等美国无良政客为谋取不正当利益,频繁登场操弄"伏特台风"虚假叙事欺骗美国国会和民众,也必将遭到美国人民对其的正义审判。 **据新华社**