悬赏通缉20名台湾嫌疑人

首次集中打击！起底台湾“资通电军”

广州市公安局天河区分局6月5日发布悬赏通告，公布中国台湾民进党当局“资通电军”指挥实施的非法网络攻击活动涉嫌多项违法犯罪，并对宁恩纬等20名参与实施网络攻击活动的重要犯罪嫌疑人进行悬赏通缉。这是公安机关首次通过执法行动对“台独”分裂势力亮剑，首次对台湾“资通电军”有组织网络违法犯罪行为的集中打击，一举查实了20名犯罪嫌疑人真实身份，全面固定犯罪证据并公开悬赏通缉。

与此同时，国家计算机病毒应急处理中心、计算机病毒防治技术国家工程实验室和360数字安全集团联合发布了《“蚍蜉撼树”——台民进党当局“资通电军”黑客组织网络攻击活动调查报告》，深度曝光“资通电军”的历史背景、组织架构、人员构成、工作地点、工作任务及网络攻击案例等信息。

据新华社、央视新闻

打击

广东警方首次悬赏通缉20名台湾“资通电军”成员

5月20日和27日，广州市公安局天河区分局先后两次发布《警情通报》，称广州某科技公司遭受网络攻击并向公安机关报案，公安机关初步查明，该公司遭受的网络攻击是台湾民进党当局“资通电军”所为。

广州市公安局天河区分局副局长纪朝平介绍，近年来，台湾“资通电军”频繁对境内不同领域机构实施无差别网络攻击活动。无底线发动网络战，图谋窃取敏感数据，向无情报价值的网络系统上传“台独”“精日”标语，煽动分裂国家，并恶意破坏网络系统正常运行，性质极其恶劣，影响这些机构的正常生产运营，涉嫌严重违法犯罪。

广州市公安局天河区分局5日正式发布《悬赏通告》，决定对宁恩纬、刘冠均、黄士恒、江致学、彭依宣等20名参与实施上述网络攻击活动的犯罪嫌疑人进行悬赏通缉，请广大群众积极提供线索，凡向公安机关提供有效线索的举报人，以及配合公安机关抓获有关犯罪嫌疑人的有功人员，将按每名犯罪嫌疑人1万元人民币的金额予以奖励。

北京大学新闻与传播学院教授，海峡两岸关系研究中心特约研究员田丽表示，这次行为是严格依法办事，依照了我国刑法、网络安全法和反间谍法。对于实行网络犯罪和这种窃取机密的行为予以通缉或是刑事追责，彰显了法律在维护网络安全方面的权威性和严肃性。她相信，以后不仅是在这些方面，对于其他的，比如散布分裂谣言的，也会依照相关法律予以追责。

起底

台湾“资通电军”已发动数千次大规模网络攻击

调查报告披露，台湾“资通电军”全称为“国防部资通电军指挥部”，其前身隶属于台湾当局“国防部老虎小组”网络部队。“资通电军”下设资讯通信处、网络作战处、电子作战处、后勤处等4个内设机构，以及1个具有培训性质的测训中心。

国家计算机病毒应急处理中心高级工程师杜振华介绍，“资通电军”是蔡英文上台后在美国军方支持下着力打造的所谓“第四兵种”，主要职责是统筹台军方“政府”，甚至民间的网络技术力量，专门针对大陆、港澳地区实施长期的网络攻击渗透。妄图窃取敏感数据和情报信息，甚至还配合美国的反华势力，对我发动舆论战、认知战，挑动、制造族群对立，妄图扰乱社会秩序，阻挠国家统一。

警方调查显示，台湾“资通电军”近年来伪装成数个黑客组织，通过漏洞扫描、密码爆破、钓鱼邮件攻击等初级网攻手法，试图窃取大陆地区的敏感数据和重要情报信息，干扰企业正常经营活动，性质极其恶劣。

公安机关调查显示，台湾“资通电军”近年来伪装成“毒云藤”“三色堇”“匿名者64”“金叶萝”“乌苏拉”等黑客组织，有组织、有计划、有预谋地对大陆和港澳地区国防军工、航空航天、政府部门、能源交通、海事、科研及科技企业等重点部门、重点领域的网络系统，实施了数千次大规模网络攻击。

通过漏洞扫描、密码爆破、SQL注入、钓鱼邮件攻击、内网嗅探、木马植入等初级网攻手法，尝试绕过目标系统安全防护措施，获取系统内网控制权限，进而窃取敏感数据和重要情报信息、干扰企业正常经营活动，性质极其恶劣，造成极为严重的社会影响。

360集团创始人周鸿祎表示，2022年，“毒云藤”（黑客组织）重点针对大陆地区科研教育相关领域，发起大规模的钓鱼邮件攻击活动。

2023年，“毒云藤”进一步扩大攻击范围，到政府机构、国防军工、交通运输领域，尤其是对机场和民用航空类的目标展开了活跃的攻击。

2024年，“毒云藤”又把攻击目标延伸到海事领域，试图窃取大陆地区海事相关的情报。

另外，台湾“资通电军”伪装的黑客组织，对大陆和港澳地区的数字媒体服务系统，以及相关网站、户外电子屏幕、网络电视等开展渗透入侵，违法上传发布大量“台独”分裂、“精日”等标语，恶意诋毁侮辱中华民族抗日英雄，借中华民族的集体伤痛取乐，挑拨离间两岸人民感情。

安天集团创始人董事长肖新光表示，目前也需要警惕这种广泛撒网、简单粗暴的攻击方式，“在这个过程中一旦他们取得重要的入口，还会发动更具隐蔽性的攻击，甚至是把所取得的线索共享给第三方的域外国家，扩大战果”。

与美情治部门合作，破坏两岸和平统一

调查报告披露，大陆技术团队通过对台湾“资通电军”的攻击活动进行追踪溯源发现，他们的攻击手段简单粗暴，为了窃取所需情报信息，甚至对于攻击源信息不做过多隐藏，因此也为大陆技术团队快速锁定相关人员提供了便利条件。

调查报告显示，台湾“资通电军”伪装的这些黑客组织，有的以网络窃密活动为主，有的以散播虚假信息为主。由于他们较多使用开源工具，因此也会留下很多攻击痕迹。

肖新光表示，从痕迹中还原出黑客组织编译程序的路径，路径中可能就包含他的用户名或项目代号；另外，有他的编译时间，这就有可能与他工作的时区相对应；还有可能带有一些他的内码字符集，这也有助于判断黑客来自哪个地区。

调查报告显示，针对不能攻破的目标系统或未窃取到有价值数据的网络平台，台湾“资通电军”网攻人员往往会恶意破坏目标系统，删除系统数据、恶意篡改数据或格式化系统存储设备等，企图干扰企业正常生产经营。

另外，据知情人士透露，台湾民进党当局长期与美国国家安全局、中央情报局等情治部门合作，配合美国“亚太战略”，妄图“倚美谋独”；美国情治部门则长期为台湾“资通电军”提供人员培训和技术装备支持，多次派出所谓“前出狩猎”团队赴台，对我开展网络攻击。

田丽表示，可以看得出来，台湾“资通电军”做这件事情不仅仅是为了自身安全，更多是与西方一些国家共享情报，甚至出卖台湾同胞和大陆同胞的利益，为获取一点点的政治资源。所以这是一个极度自私、恶劣和卑贱的行为。他们的技术并不先进，带有非常强的挑衅性，希望通过挑动大陆对他进行反击，以此来刺激两岸民众的对立情绪，绑架民众的政治立场，这个行为是极其恶毒的。

相关新闻

国台办宣布

对“台独”顽固分子沈伯洋关联企业予以惩戒

国务院台办发言人朱凤莲5日表示，经查，“台独”顽固分子沈伯洋之父沈土城在台湾企业兆亿有限公司担任负责人，该公司与大陆某些企业存在贸易往来与业务合作，从中谋取经济利益。大陆方面决不允许“台独”顽固分子关联企业在大陆谋利，决定对兆亿有限公司实施惩戒，禁止其与大陆组织、企业、个人进行任何交易、合作，并将对其采取其他必要措施。 据新华社