2025年6月6日 星期五 齐鲁晚报

起底台湾『资通电军』如何被快速锁定

悬赏通缉！20名台湾民进党当局『资通电军』首要嫌犯曝光

记者6月5日从广州警方获悉，针对台湾民进党当局相关的黑客组织对大陆实施的非法网络攻击活动，涉嫌多项违法犯罪，5日，广州市公安局天河区分局正式发布《悬赏通告》，决定对宁恩纬等20名参与实施网络攻击活动的首要犯罪嫌疑人进行悬赏通缉。他们是如何犯罪的？台湾“资通电军”网络攻击手段有哪些？警方是如何快速锁定境外“黑手”的？

广州某科技公司连续遭两次网络攻击

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表示，公安机关深入侦查发现，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。

为依法打击恶意网络攻击和非法控制、破坏计算机信息系统犯罪，切实维护国家安全、人民群众生命财产安全及合法权益，广州市公安局天河区分局正式发布《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》。对于我国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，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”黑客组织网络攻击活动

针对台湾黑客组织对大陆进行的网络违法攻击活动，国家计算机病毒应急处理中心等机构5日联合发布了《台民进党当局“资通电军”黑客组织网络攻击活动调查报告》，曝光了台湾“资通电军”的组织架构、人员构成、工作任务等信息，以及阻挠国家统一的行径。

据调查报告披露，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表示，“资通电军”是2017年台湾民进党当局成立的所谓“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。

据警方调查显示，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。

台湾“资通电军”攻击手段

●近年来，伪装成“毒云藤”“三色堇”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

●针对其不能攻破的目标系统或未窃取到有价值数据的网络平台

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

据人民日报

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，试图窃取大陆地区与海事相关的情报。

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。

近年来，台湾“资通电军”通过伪装的数个黑客组织，对大陆和港澳地区重点部门、重点领域的网络系统实施了数千次大规模网络攻击。

安天集团创始人董事长肖新光表示，目前需要警惕黑客组织采取广泛撒网、简单粗暴的攻击方式。在这个过程中，一旦他们取得重要入口，可能还会发动更具隐蔽性的攻击，甚至把取得的线索共享给第三方的域外国家，由他们再去扩大战果。所以，虽然我们看到他们的组织攻击水平不高，但还是要更加提高警惕。

攻击手法简单粗暴 为快速锁定提供条件

据调查报告披露，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。据调查报告显示，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。

据网络安全专家介绍，台湾黑客组织实施的网络攻击具有明显的政治背景，具有高度定向性，属于典型的APT攻击。那什么是APT攻击呢？涉案的台湾黑客组织是怎么被精准锁定的呢？国家计算机病毒应急处理中心高级工程师杜振华介绍，APT攻击直译过来叫高级持续性威胁攻击，具体体现在它使用的漏洞，可能是一些利用难度比较大的漏洞，甚至是未知的漏洞。使用的这些木马病毒和网络武器，通常是自主开发的。攻击者在目标选择上，相较于普通网络攻击的随机性、发散性而言，对目标的选择专注度更高，可能对同一目标实施数月甚至长达数年的持续性攻击。

不同于普通网络攻击的“广撒网”模式，APT攻击如同训练有素的“网络间谍”，往往提前数月甚至数年锁定目标。他们利用零日漏洞、钓鱼邮件等手段，悄无声息地渗透系统、长期潜伏，进而窃取目标单位的重要数据。

然而，据网络安全专家介绍，通过相关网络攻击样本和攻击手法分析，涉案的台湾黑客组织技术水平整体较低，攻击手法简单粗暴，攻击范围较广，多次被我网络防护系统监测发现。肖新光表示，从痕迹中会还原出黑客组织编译程序的路径，在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。

据调查报告显示，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。

与美情治部门合作 破坏两岸和平统一

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”做这件事情的目的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。

据央视新闻

新华时评

对“台独”分裂势力挑衅零容忍、不姑息

5日，大陆公安机关依法公开通缉台湾“资通电军”重要犯罪嫌疑人，国台办宣布对“台独”顽固分子沈伯洋关联企业予以惩戒。一日两记重拳形成有力打击和强大震慑，再次彰显大陆对“台独”分裂势力挑衅零容忍、不姑息的坚定立场、坚决态度。

当日公布的惩戒措施合法合规，精准有力。相关举措既是对“台独”分裂势力的严正警告和有力震慑，有助于维护国家主权、安全、发展利益，维护两岸同胞根本利益，也展现大陆方面不断升高反对和遏制“台独”力度、精准度，将进一步有效切断“台独”顽固分子的“金脉”，有利于进一步打击“台独”分裂活动，遏制“台独”分裂势力与外部势力勾连图谋。

统一是正道，“台独”是绝路。希望广大台胞台企认清“台独”的极端危险性、危害性，站在历史正确的一边，以实际行动与“台独”分裂势力划清界限，多做维护和推动两岸关系和平发展的事，与大陆同胞携手坚决反对“台独”分裂行径，守护中华民族共同家园，共创两岸同胞绵长福祉。

据新华社

编辑：武俊 美编：杨晓健 组版：刘淼

报料电话：13869196706 欢迎下载齐鲁壹点 600多位在线记者等你报料

报纸发行：(0531)85196329 85196361 报纸广告：(0531)85196150 85196192 文字差错投诉：(0531)85193436 发行投诉：4006598116 (0531)85196527 邮政投递投诉：11185 全省统一零售价：1.5元

邮发：23-55 广告许可证：鲁工商广字01081号 地址：济南泺源大街2号 大众传媒大厦 邮编：250014 大众华泰印务公司(大众日报印刷厂)印刷(济南市长清区玉皇山路1678号)