广州某科技公司遭境外黑客网攻 系民进党当局豢养的黑客组织所为

网络安全专家称，涉案台湾黑客组织技术水平较低，手法简单粗暴

昨天，记者从广州市公安局天河区分局了解到，广州某科技公司遭境外黑客组织网络攻击事件发生后，公安机关立即组织技术团队对提取的攻击程序和系统日志进行技术分析和溯源追踪，初步查明该公司遭受的网络攻击系中国台湾民进党当局豢养的黑客组织所为。

公安机关接到报警后，第一时间固定证据，提取相关攻击程序样本。

周鸿祎

黑客组织采用常规攻击手段 属初级APT攻击

据广州市公安局天河区分局5月20日发布的警情通报显示，广州某科技公司自助设备的后台系统在遭受网络攻击后，被违法上传了多份攻击程序，恶意破坏系统正常运行。事件发生后，该公司立即启动应急预案，第一时间尝试恢复系统，并向当地公安机关报案。

广州市公安局天河区分局办案民警李雲鹏介绍说：“公安机关接到报警后，第一时间固定证据，提取相关攻击程序样本。经技术分析发现，该案属于初级APT攻击，采用的是常规攻击手段，即利用开源扫描工具，对我境内特定IP地址段实施无差别扫描探测。发现存有漏洞的计算机信息系统，再利用漏洞入侵到该系统，获取系统管理员权限，进而控制相关单位所有前端设备，并上传恶意代码。”

根据公安机关掌握的情况，广州某科技公司的部分设备和系统在遭到了恶意破坏后，导致较长时间服务中断，影响了企业的正常生产运营，同时该受害企业下架了部署的设备，给企业造成了一定经济损失。

广州市公安局天河区分局副局长纪朝平说：“针对该起黑客攻击案件，公安机关组织专业技术团队全面开展技术溯源工作，通过对攻击者暴露的大量网络线索进行系统梳理、深入分析，成功锁定了具有中国台湾当局政府背景的网络黑客组织，提取固定了大量电子证据。下一步公安机关将继续对该黑客组织及其骨干成员开展侦查调查，查清犯罪事实，依法严厉打击相关犯罪嫌疑人。”

台湾黑客组织 网络攻击大陆上千个重要目标

据记者了解，专业技术团队通过对警方提取的相关攻击程序样本进行分析发现，此次网络攻击是台湾民进党当局策划的一次有组织、有预谋的大规模网络攻击行动，并且带有明显的网络战痕迹。

据警方调查掌握，该台湾黑客组织近年来频繁利用公开网络资产探测平台，针对大陆10余个省份的1000余个重要网络系统，涉及军工、能源、水电、交通、政府等领域开展大规模网络资产探查。

国家计算机病毒应急处理中心高级工程师杜振华介绍，“首先是通过网络端口的探测扫描，去发现目标单位暴露在互联网上网络资产的一些基本信息。同时还通过搜索引擎或公开信息检索等手段，去搜集目标单位以及相关工作人员的联系方式，比如电子邮件。如果没有合适的漏洞，可能会采用社会工程学的攻击方式，向相关的工作人员发送钓鱼网站链接，窃取相关工作人员的用户名口令。一旦运行之后可能会进入到目标单位的内网，再进一步进行探测和入侵。”

360集团创始人周鸿祎说：“在过去的这10年里，我们收集了全世界将近400亿个病毒木马和攻击者的样本。像台湾地区的这几个APT组织，我们一共发现了可能来自5家不同的团队，他们的编程手法、代码特征、攻击习惯基本上都在我们的知识库里。所以只要一对照，基本上就水落石出了。”

根据技术团队分析显示，虽然该黑客组织频繁利用VPN代理、境外云主机和傀儡机等网络资产，通过大量来自美国、法国、韩国、日本、荷兰、以色列、波兰等国家的IP地址实施网络攻击，意图掩盖其真实攻击来源，但通过网络侦查调查，不难查清该黑客组织实施网络攻击犯罪的整个过程及其真实意图。

杜振华表示，“这些攻击一方面反映出攻击者试图通过这种攻击对我（大陆）实施袭扰、骚扰和干扰，另一方面也反映出攻击者正在试图去获取我（大陆）境内的这些网络资产的控制权，为后续的攻击或者进一步的攻击，准备相应的跳板机和傀儡机，用心非常险恶。”

涉案台湾黑客组织 技术水平较低

据网络安全专家介绍，此次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？

杜振华介绍说：“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。

安天集团创始人、董事长肖新光说：“首先，他们比较多使用商用的或开源的木马或者工具，一定程度上说明他们缺少自研工具的能力；第二，他们极少出现使用零日漏洞的相关情况，说明他们缺少这方面的储备；第三，他们整个攻击活动是比较泛化的，也就是撒大网捞鱼，这就使他们的攻击本身是比较容易被发现和暴露的。”

周鸿祎说：“台湾地区的几个APT组织简单而粗暴，能力属于三流团队水平，也没有太多的掩饰和隐藏。他们的攻击特征，从现在他们攻击的对象和窃取的情报来看，具有强烈的政治意义目的，他们比较偏重于国防和外交等方面的情报和信息窃取。”

据新华社、央视

新闻链接

如何防范 网络攻击威胁？

据网络安全专家介绍，这些具有高度定向、持续性的APT攻击是目前网络安全最大的威胁，那么能采取哪些安全措施进行防御呢？杜振华介绍了三项措施：

首先，相关单位和个人要按照我国网络安全相关的法律法规和标准规范，落实网络安全防范的各项措施。

第二，尽量避免或者杜绝犯一些低级错误，比如弱口令，口令设置非常简单，或者使用默认口令或长期口令不修改等；再比如一些已知高危漏洞，长时间不进行修补。这些都是非常容易被攻击者利用，也非常容易出现的一些问题。

第三，尤其要注意电子邮件的安全，特别是防范钓鱼邮件，原则是多联系多核实。有一些常见钓鱼邮件的攻击套路，像伪造的会议通知、邀请函、约稿通知、论文录用通知等，都是非常常见的、攻击者会用到的套路，需要相关单位和相关人员提高防范意识。

网络安全专家提醒，如果遇到异常登录提醒、系统性能突变等异常情况，要提高安全防范意识，及时启动应急响应机制，并立即向相关部门上报威胁信息。

南方今年以来最强暴雨来袭 可达大暴雨级别

注意啦！今年以来强度最强，暴雨、大暴雨范围最大的新一轮降水已于昨日夜间开始登场，并将在接下来两天横扫南方大部地区。此次降水单日降雨量大，局地降雨具有极端性，且强降雨落区与上一轮高度重叠，致灾风险高，需高度警惕！

此轮强降雨有何特点？

1.强度强！暴雨或大暴雨成过程“标配”。

从过程来看：27日夜间南风增强、低涡切变建立，降雨明显增强；28日为过程最强时段；29日夜间减弱。

从累计降雨量来看：27日至29日，贵州、江南、华南大部地区有大到暴雨，江南南部、华南北部部分地区大暴雨，局地特大暴雨，江南南部、华南北部累计雨量可达100~180毫米，局地250~300毫米。

除了累计雨量大，还需警惕短时强降雨伴随出现。从降水特点来看：贵州、江南南部和东部等地以混合性降水为主，持续时间长、范围大、累计雨量较大。两广、福建东南部等地主要为暖区对流，降雨强度大，较为分散，局地短时降雨强度可达80毫米以上。

2.范围大！暴雨将覆盖长江以南大部地区。具体来看，28日进入降雨最鼎盛时段，大到暴雨范围覆盖广西、广东、湖南、江西、福建、浙江等多个省区，其中江西、福建局地有大暴雨；28日夜间大到暴雨向东、向南缩减。29日江南、华南强降雨陆续结束，台湾岛仍有暴雨。

为何这次降水如此强？

气象分析师叶梦龙解释，此次强降雨主要由低涡切变线逐步发展东移导致，同时孟加拉湾和南海的两支偏南气流向南方输送水汽，叠加低空偏东风水汽，水汽条件非常好。动力与水汽条件的共同作用，导致南方出现今年以来最强降雨过程。

据央视新闻

新闻链接

降雨今日逐步结束

昨天白天，重庆大部地区小到中雨，偏南部分地区大到暴雨；武隆、彭水、酉阳3个区县的9个雨量站达暴雨，最大雨量74.0毫米，大部分地区气温17℃～27℃。根据预计，28日白天，降雨逐渐结束；28日夜间到30日白天，各地以多云为主。

天气预报

28日白天，东北部和偏西地区多云，其余地区阵雨，气温15℃～31℃；中心城区阵雨，气温21℃～28℃。

28日夜间到29日白天，各地多云到晴，气温14℃～34℃；中心城区多云到晴，气温21℃～31℃。

29日夜间到30日白天，大部地区多云转阴天，局地有阵雨，气温13℃～33℃；中心城区多云转阴天，气温22℃～32℃。新重庆-上游新闻

山东高密化工厂爆炸事故 致5人死亡6人失联

据新华社电 记者从山东省高密市应急管理局获悉，27日11时57分左右，高密市友道化学有限公司一车间发生爆炸事故。经各级组织力量全力搜救，截至19时25分，事故造成5人死亡，6人失联，19人轻伤。

事故发生后，山东省委、省政府高度重视，立即作出安排部署，省、市、县三级启动应急处置机制，成立联合救援指挥部，全力组织开展救援，全面做好失联人员搜救、伤员救治、家属安抚、善后处置、环境监测等各项工作。目前现场搜救和清理工作仍在进行中。

据悉，应急管理部有关负责人已率工作组赶赴事故现场。应急管理部调派国家综合性消防救援力量、国家安全生产专业救援力量前往增援，协调医疗卫生专家参与伤员救治。