长期窃取我国敏感数据，29个海外黑客组织被曝光

发布时间：2016-01-19 12:08:15 来源：中国经济网 作者：佚名 责任编辑：王磊

日前，360天眼实验室发布了《2015年中国高级持续性威胁（APT）研究报告》。报告显示，中国作为高级持续性威胁（APT）攻击的主要受害国，仅2015就已发现29个针对中国境内机构进行APT攻击的黑客组织。这些APT组织长时间潜伏，有的网络间谍活动最长持续8年之久。黑客组织从中国科研、政府机构等领域窃取了大量敏感数据，对国家安全已造成严重的危害。其中，中国的教育科研、政府机构、能源、军事等行业是遭受攻击的重灾区。

《2015年中国高级持续性威胁（APT）研究报告》是对目前针对中国的APT攻击组织的年度总结。主要内容包括：

中国是高级持续性威胁（APT）攻击的主要受害国。截至2015年11月底，360天眼实验室监测到的针对中国境内科研教育、政府机构等组织单位发动APT攻击的境内外黑客组织累计29个，其中15个APT组织曾经被国外安全厂商披露过，另外14个为360天眼实验室首先发现并监测到的APT组织，其中包括2015年5月末发布的海莲花（OceanLotus）APT组织。

北京、广东是重灾区教育科研与政府机构是主要遭攻击领域。国内多个省市受到不同程度的影响，其中北京、广东是重灾区。国内受影响量排名前五的省市是：北京、广东、浙江、江苏、福建等沿海相关省市。受影响量排名最后的五个省市是：西藏、青海、宁夏、新疆、贵州。

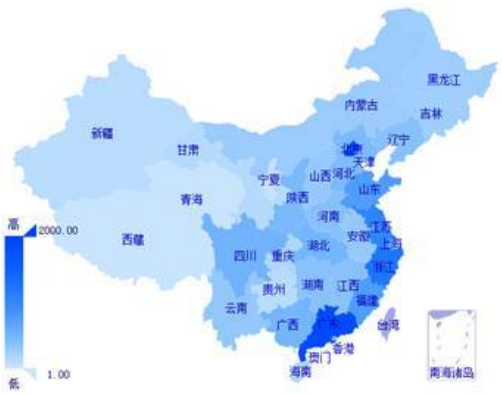


图1国内受影响情况（2014年12月-2015年11月）

教育科研、政府机构是APT攻击主要针对的领域。其他受到攻击的行业还包括能源、军事、工业与商业等。科研与教育机构能够成为2015年APT攻击的首要目标，在一定程度上反映出境外APT组织对中国科技情报的“兴趣”。几乎所有境外APT组织都会将中国的政府机构列入自己的战略攻击目标。这说明绝大多数的APT组织都是具有政府背景的。

互联网

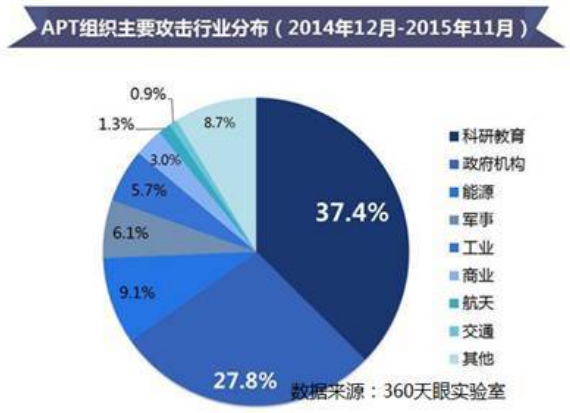
- 世纪之赌两周年：雷军未达预期 董明珠继续造梦
- 广州33天内清理超10万辆网约车
- 美团点评或完成33亿美元融资 估值达180亿美元
- 发力硬件业务 360欲为回归A股高估值铺路
- 清华教学门户网站遭黑客攻击


孙俪拥萌犬登封面


热心人赠环卫阿姨雨鞋驱寒意


4米高萌猴造型“生气小子”亮相上海


医院咖啡馆投入运营 不以营利为目的



攻击持续时间长，最长可达8年

攻击者长期持续对特定目标进行精准的打击。在这29个APT组织中，针对中国境内目标的攻击最早可以追溯到2007年，该组织主要针对中国政府、军事、科技和教育等重点单位和部门，相关攻击行动最早可追溯到2007，至今还非常活跃。也就是从2007年开始进行了持续8年的网络间谍活动。最近三个月（2015年9月以后）内仍然处于活跃状态的APT组织至少有9个。

我国相关机构防御薄弱低成本攻击频频得手

针对中国的APT攻击主要由低成本的攻击组成，但由于相关防御薄弱导致低成本攻击频频得手。研究人员发现，针对中国的攻击中，APT组织更多选择1day或Nday等已知漏洞，这说明相关机构对曝出的漏洞并未及时修补，安全意识较差。此外，邮件攻击是APT攻击中使用最为频繁的攻击载体。针对中国的鱼叉邮件攻击主要是携带可执行程序，这也从侧面反应出中国相关机构的安全防御措施、以及人员的安全意识比较欠缺。

大量敏感数据被窃取，国家安全遭受严重危害

APT组织从中国科研、政府机构等领域窃取了大量敏感数据，对国家安全已造成严重的危害。其中名为APT-C-05的组织是一个针对中国攻击的境外APT组织，也是至今捕获到针对中国攻击持续时间最长的组织。APT组织窃取的具体数据内容有很大差异，但均涉及中国科研、政府等领域的敏感数据，其中窃取的敏感数据中以具备文件实体形态的文档数据为主，进一步会包括账号密码、截图等。窃取的敏感数据主要以文档为主，APT组织更关注WPS Office相关文档。WPS Office办公软件的用户一般分布在国内政府机构或事业单位。

攻击紧密围绕政济、科技、军工等热点领域

十三五规划、一带一路、军工制造等内容是APT组织关注的重点领域。国民经济和社会发展第十三个五年规划纲要（2016－2020年，简称“十三五”规划）是2016年－2020年中国经济社会发展的宏伟蓝图。稳步推进“一带一路”建设合作是中国“十三五”规划的重要内容。在2015年11月、12月期间，研究人员已捕获到针对相关目标的攻击行动，相关攻击行动主要以“一带一路”、“21世纪海上丝绸之路”等诱饵信息攻击相关领域的目标群体。

360企业安全集团总裁吴云坤表示，从本次报告的结果看，国内科研与政府等相关机构的安全防御措施亟待加强，工作人员的网络安全意识比较淡薄。在帮助政企用户加强网络安全防护上，国内安全厂商还有很多工作要做。

这是继2015年5月发布"海莲花"分析报告后，360天眼实验室第二次发布APT相关研究报告。据360天眼实验室负责人韩永刚透露，2016年360天眼实验将会持续发布APT相关报告，报告全文可以在360威胁情报中心（TI.360.com）下载浏览。

成立于2014年的360天眼实验室致力于利用大数据技术研究未知威胁。该实验室旗下的天眼系统(SkyEyeSystem)是全球首个基于大数据的未知威胁感知系统。

1 李彦宏回应“贴吧事件” 称公司将会深刻反省
2 联想移动再变阵：陈旭东挂帅 任伟光空降加盟
3 金亚科技自曝多项财务造假
4 VR烧向消费级市场：技术破冰 内容限制
5 校讯通成学校运营商谋利工具 专家建议取消
6 罗永浩：为什么中国人如此在意性价比？
7 智联招聘郭盛：程序员行业需求强劲 供给不足
8 在深圳创业 这六项补贴记得申请
9 电商下乡面临成长烦恼：产品利润薄甚至亏损
10 国美话费充值系统漏洞：三男子盗窃23万元话费

热点专题
- 保险周刊第90期
- 北京市发文规范汽车租赁市场
- 基金周刊第127期
- 大智慧收购湘财证券 或成首家互联网券商
- 股事绘第8期：淘金港股通（一）
- 统一企业陷亏损泥潭

高清图集

大电池+金属机身 红米手机3图赏

售价2999元 360奇酷手机极客版真机图赏

CES 2016现场图赏