#### 毒云藤

**别称:**

“绿斑”（Green Spot）

**可能操作来源:**

台湾、香港、美国

**目标:**

中国：集中在北京、福建、广东、浙江、上海。

**(CFR) 事件类型:**

间谍行为

**组织简介:**

毒云藤组织对中国国防、政府、科技、教育以及海事机构等重点单位和部门进行了长达 11 年的网络间谍活动。该组织主要关注军工、中美关系、两岸关系和海洋相关领域，其关注的领域与我们之前发布的海莲花（OceanLotus）APT 组织有一定相似的地方。 360 追日团队捕获毒云藤的首个木马出现在 2007 年 12 月。

该组织在初始攻击环节主要采用鱼叉式钓鱼邮件攻击，攻击之前对目标进行了深入调研和精心挑选，选用与目标所属行业或领域密切相关的内容构造诱饵文件和邮件，主要是采用相应具体领域相关会议材料、研究成果或通知公告等主题。期间漏洞文档样本数量 10 个，其中包含 1 个 0day 漏洞。这些木马的感染者遍布中国境内 31 个省级行政区。

**参考链接:**

* <https://www.freebuf.com/column/185149.html>
* <https://www.antiy.cn/research/notice&report/research_report/20180919.html>