#### 海莲花

**别称:**

SeaLotus，OceanLotus，APT-C-00

**可能操作来源:**

越南

**目标:**

对中国政府、科研院所、海事机构、海域建设、航运企业等相关领域

**(CFR) 事件类型:**

间谍行为

**组织简介:**

2012 年 4 月起，OceanLotus组织对中国政府、科研院所、海事机构、海域建设、航运企业等相关重要领域展开了有组织、有计划、有针对性的长时间不间断攻击。

该组织主要通过鱼叉攻击和水坑攻击等方法，配合多种社会工程学手段进行渗透，向境内特定目标人群传播特种木马程序，秘密控制部分政府人员、外包商和行业专家的电脑系统，窃取系统中相关领域的机密资料。

2014 年 2 月以后，OceanLotus 进入攻击活跃期，并于 2014 年 5 月发动了最大规模的一轮鱼叉攻击，大量受害者因打开带毒的邮件附件而感染特种木马。而在 2014 年 5 月、9 月，以及 2015 年 1 月，该组织又对多个政府机构、科研院所和涉外企业的网站进行篡改和挂马，发动了多轮次、有针对性的水坑攻击。

OceanLotus 组织的攻击周期之长（持续 3 年以上）、攻击目标之明确、攻击技术之复杂、社工手段之精准，都说明该组织绝非一般的民间黑客组织，而很有可能是具有国外政府支持背景的、高度组织化的、专业化的境外国家级黑客组织。

**参考链接:**

* <https://portswigger.net/daily-swig/apt32-unmasked-researchers-shine-light-on-the-notorious-hacking-group-targeting-southeast-asian-businesses>
* <https://threatpost.com/oceanlotus-apt-uses-steganography-to-shroud-payloads/143373/>
* <https://www.welivesecurity.com/wp-content/uploads/2018/03/ESET_OceanLotus.pdf>
* <https://unit42.paloaltonetworks.com/tracking-oceanlotus-new-downloader-kerrdown/>
* <https://www.scmagazineuk.com/ocean-lotus-group-apt-32-identified-vietnamese-apt-group/article/1474614>
* <https://www.freebuf.com/news/topnews/68622.html>