

**海莲花介绍：**

海莲花(OceanLotus、APT32)是一个具有越南背景的黑客组织。该组织最早被发现于2012年4月攻击中国海事机构、海域建设部门、科研院所和航运企业。主要使用鱼叉和水坑攻击方式，配合社工手段，利用特种木马进行窃密活动。2014年开始，其活动强度加大。

海莲花高强度的攻击自2014年起持续至今，攻击目标越来越明确、攻击技术越来越复杂、社工手段越来越精准、与杀毒软件的对抗性与防溯源的隐蔽性越来越强。海莲花的技术手段表明其已发展为一个高度组织化、专业化的境外国家级黑客组织。

海莲花的攻击目标与越南存在较大联系，遍布政治、经济、社会等多个重要领域。具有较明确的窃取机密文件的目的。

<http://threatrecord.com/hai-lian-hua-oceanlotus-apt32/>

**部分相关样本：**

1. OceanLotus Tester（2012）

OceanLotus Encryptor（2014.2）

OceanLotus MAC（2014.11）

OceanLotus Cloudrunner（2014.2）

来自360

<http://www.freebuf.com/news/topnews/68622.html>

1. WINDSHIELD（2014-2016）

KOMPROGO（2016）

SOUNDBITE（2016）

PHOREAL（2016）

BEACON (Cobalt Strike)（2016）

来自fireeye

<https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html>

1. Framework A, B（2017.11.6）

来自volexity

<https://www.volexity.com/blog/2017/11/06/oceanlotus-blossoms-mass-digital-surveillance-and-exploitation-of-asean-nations-the-media-human-rights-and-civil-society/>

1. 一次利用office恶意宏的分析（2017.9.2）

来自微步

<https://mp.weixin.qq.com/s?__biz=MzI5NjA0NjI5MQ==&mid=2650164408&idx=1&sn=a5abc26a34f4f21c20619146686670bf&chksm=f448b704c33f3e12b82011b989c89de83376c224341fd00583811f98ab399f3d4665de64b5d8&scene=38#wechat_redirect>

1. Denis（2017.11.23）

来自微步

<https://mp.weixin.qq.com/s?__biz=MzI5NjA0NjI5MQ==&mid=2650164579&idx=1&sn=6f73321ba3b6f41c085750fcade2fe6b&chksm=f448b6dfc33f3fc9eac6fba309d5c386058e69cf1671afdc71ddac5b12d8435058dd88694a88&scene=38#wechat_redirect>

1. 一次利用office漏洞投递Denis的分析（2018.5.6）

来自微步

<https://mp.weixin.qq.com/s?__biz=MzI5NjA0NjI5MQ==&mid=2650164761&idx=1&sn=2706219e9cb0010ae93d56789ed44a1b&chksm=f448b5a5c33f3cb31ba9402810a10376d7d729352b17de2d62e62811ec06fcd0d4d2a1998ea3&scene=38#wechat_redirect>

1. 微步对最新的windows、macOS样本进行的分析（2018.9.10）

来自微步

<https://mp.weixin.qq.com/s?__biz=MzI5NjA0NjI5MQ==&mid=2650164993&idx=1&sn=6de7c4d67c75c772e15ad3ca24ba70b4&chksm=f448b4bdc33f3dab8785fdb95d1f3432de63acbfeb868ae02bad805f50ac6dea1f584de2fed2&scene=38#wechat_redirect>

1. MacOS后门程序（2017.7.1）

来自PALO ALTO NETWORKS

<https://www.easyaq.com/news/103458664.shtml>（来源于PALO ALTO NETWORKS）

1. 利用永恒之蓝针对高校的攻击（2018.9.12）

来自360

<https://www.anquanke.com/post/id/159555>

1. 利用MSBuild机制免杀样本分析（2017.11.23）

来自360

<https://mp.weixin.qq.com/s/3v_dGXGZ_RkVyMxl6s3MIg>

1. 漏洞利用类攻击样本分析（2017.12.1）

来自360

<https://mp.weixin.qq.com/s/IPFKLRZb5GDXXGHioPu4RA>

**溯源技术与流程：**

选取容易分析的案例，分析溯源过程和技术手段

1. 攻击主机的溯源取证
2. 控制主机的溯源取证
3. 攻击者及组织溯源取证
   1. 恶意代码样本分析
   2. 攻击行为模式分析
   3. 攻击组织刻画
      1. 组织代号汇总
      2. 组织来源地域
      3. 组织主要目标和意图
      4. 组织常用攻击方法
      5. 攻击事件汇总

**溯源结果评价：**

对以上分析的溯源过程和技术手段进行评价

1. 溯源方法评价
2. 结果可信度评估

**攻击和溯源复现**