APT

OceanLotus (APT-C-00)

数字海洋的游猎者

持续3年的网络空间威胁

SkyEye
天眼实验室

摘要

- 2012 年 4 月起，有境外黑客组织对中国政府、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。我们将其命名为 OceanLotus。
- 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。
- 现已捕获 OceanLotus 特种木马样本 100 余个，感染者遍布国内 29 个省级行政区和境外的 36 个国家。其中，92.3%的感染者在中国。北京、天津是国内感染者最多的两个地区。
- 为了隐蔽行踪，该组织还至少先后在 6 个国家注册了 C2（也称 C&C，是 Command and Control 的缩写）服务器域名 35 个，相关服务器 IP 地址 19 个，服务器分布在全球 13 个以上的不同国家。
- 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 先后使用了 4 种不同形态的特种木马。初期的 OceanLotus 特种木马技术并不复杂，比较容易发现和查杀。但到了 2014 年以后，OceanLotus 特种木马开始采用包括文件伪装、随机加密和自我销毁等一系列复杂的攻击技术与安全软件进行对抗，查杀和捕捉的难度大大增加。而到了 2014 年 11 月以后，OceanLotus 特种木马开始使用云控技术，攻击的危险性、不确定性与木马识别查杀的难度都大大增强。
- 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。

关键词：OceanLotus、APT、鱼叉攻击、水坑攻击

OceanLotus 概述

2012 年 4 月起至今，某境外黑客组织对中国政府、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。

根据该组织的某些攻击特点，我们将其命名为 OceanLotus。

目前已经捕获的与 OceanLotus 相关的第一个特种木马出现在 2012 年 4 月。在此后的 3 年中，我们又先后捕获了与该组织相关的 4 种不同形态的特种木马程序样本 100 余个，这些木马的感染者遍布国内 29 个省级行政区和境外的 36 个国家。此外，为了隐蔽行踪，该组织还至少先后在 6 个国家注册了用于远程控制被感染者的 C2（也称 C&C，是 Command and Control 的缩写）服务器域名 35 个，相关服务器 IP 地址 19 个，服务器分布在全球 13 个以上的不同国家。

从 OceanLotus 发动攻击的历史来看，以下时间点和重大事件最值得关注：

1） 2012 年 4 月，首次发现与该组织相关的木马。OceanLotus 组织的渗透攻击就此开始。但在此后的两年左右时间里，OceanLotus 并不活跃。

2） 2014 年 2 月，OceanLotus 开始通过鱼叉攻击的方法对我们国内目标发起定向攻击，OceanLotus 进入活跃期，并在此后的 14 个月内对我国多个目标发动了不间断的持续攻击。

3） 2014 年 5 月，OceanLotus 对国内某权威海洋研究机构发动大规模鱼叉攻击，并形成了过去 14 个月中鱼叉攻击的最高峰。

4） 同样是在 2014 年 5 月，OceanLotus 还对国内某海洋建设机构的官方网站进行了篡改和挂马，形成了第一轮规模较大的水坑攻击。

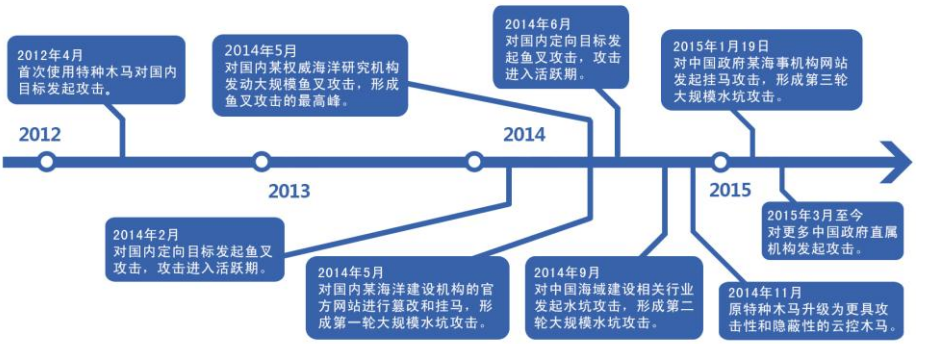
5） 2014 年 6 月，OceanLotus 开始大量向中国渔业资源相关机构团体发鱼叉攻击。

6） 2014 年 9 月，OceanLotus 针对于中国海域建设相关行业发起水坑攻击，形成了第二轮大规模水坑攻击。

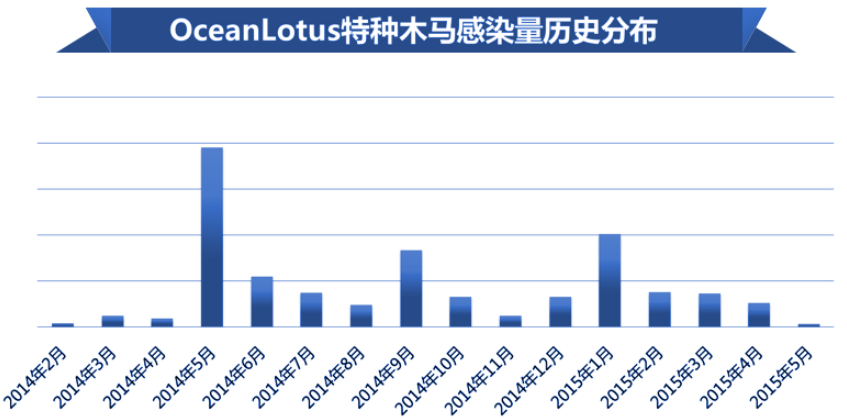
7） 2014 年 11 月，OceanLotus 开始将原有特种木马大规模的更换为一种更具攻击性和隐蔽性的云控木马，并继续对我国境内目标发动攻击。

8） 2015 年 1 月 19 日，OceanLotus 针对中国政府某海事机构网站进行挂马攻击，第三轮大规模水坑攻击形成。

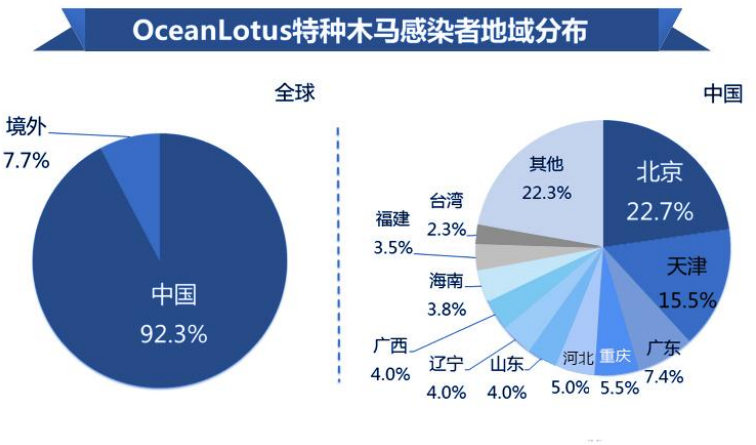
9） 2015 年 3 月至今，OceanLotus 针对更多中国政府直属机构发起攻击。



通过对 OceanLotus 组织数年活动情况的跟踪与取证，我们已经确认了大量的受害者。下图为 2014 年 2 月至今，全球每月感染 OceanLotus 特种木马的电脑数量趋势分布。



从地域分布上看，OceanLotus 特种木马的境内感染者占全球感染总量的 92.3%。而在境内感染者中，北京地区最多，占 22.7%，天津次之，为 15.5%。



下图为境内 OceanLotus 特种木马感染者数量地域分布图。

技术分析显示，初期的 OceanLotus 特种木马技术并不复杂，比较容易发现和查杀。但到了 2014 年以后，OceanLotus 特种木马开始采用包括文件伪装、随机加密和自我销毁等一系列复杂的攻击技术与安全软件进行对抗，查杀和捕捉的难度大大增加。而到了 2014 年 11 月以后，OceanLotus 特种木马开始转向云控技术，攻击的危险性、不确定性与木马识别查杀的难度都大大增强。

综合来看，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。