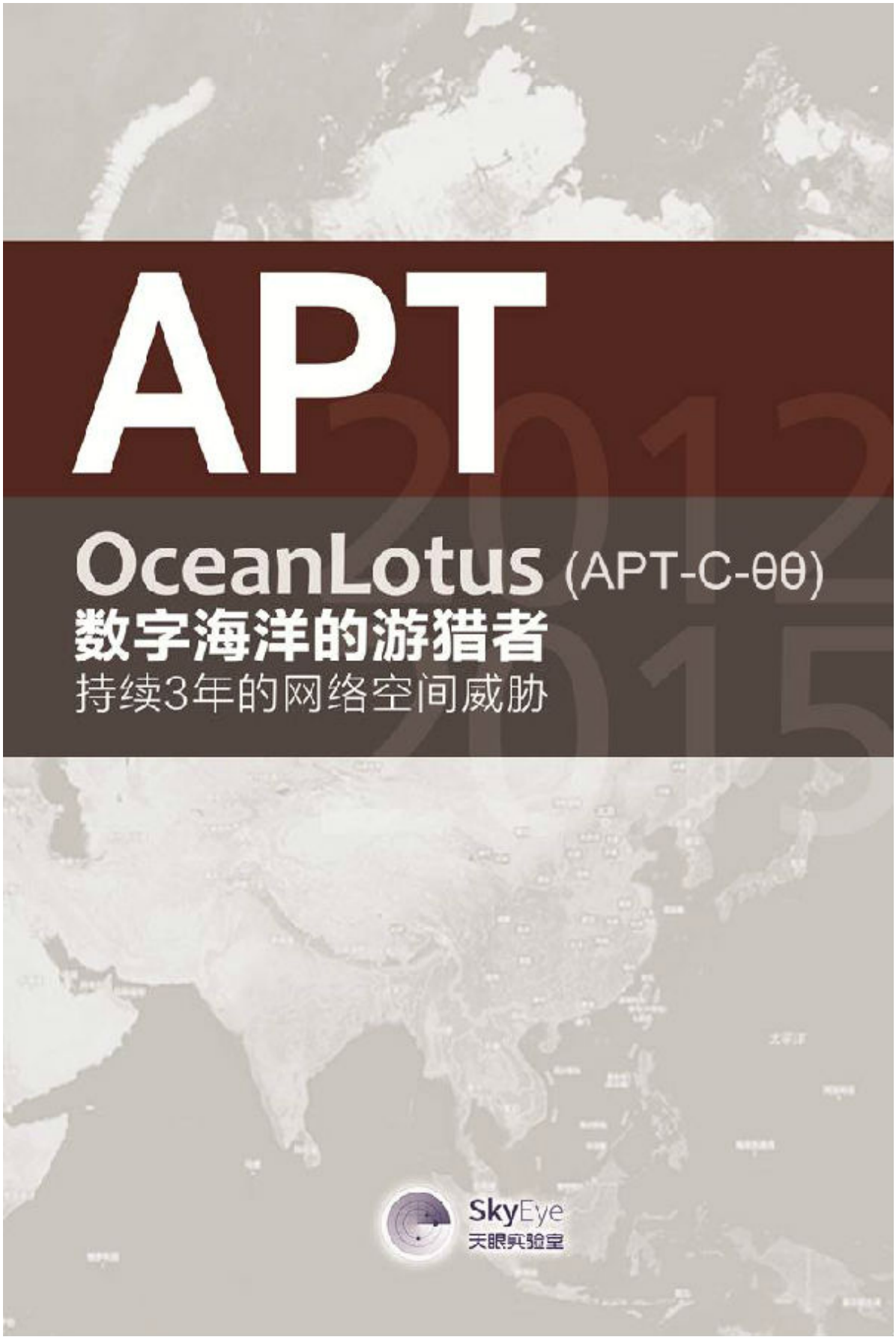
“海莲花”APT报告：攻击中国政府海事机构的网络空间威胁

May 28, 2015 • 360安全卫士



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

第一章 OceanLotus**概述**

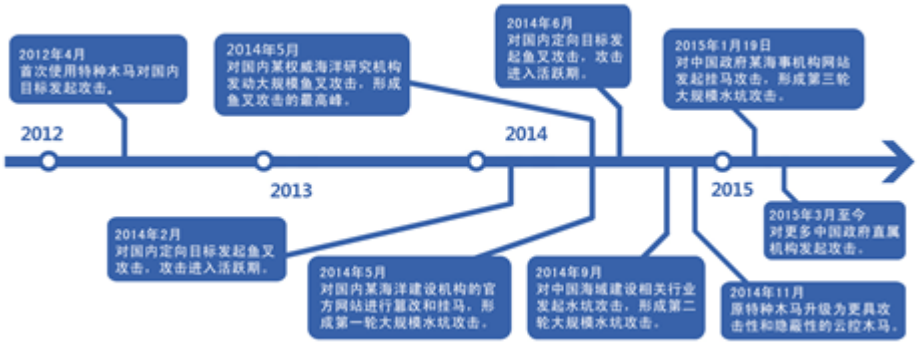
2012年4月起至今，某境外黑客组织对中国政府、科研院所、海事机构、海域建设、航运企业等相关重要领域展开了有组织、有计划、有针对性的长时间不间断攻击。该组织主要通过鱼叉攻击和水坑攻击等方法，配合多种社会工程学手段进行渗透，向境内特定目标人群传播特种木马程序，秘密控制部分政府人员、外包商和行业专家的电脑系统，窃取系统中相关领域的机密资料。

根据该组织的某些攻击特点，我们将其命名为OceanLotus。

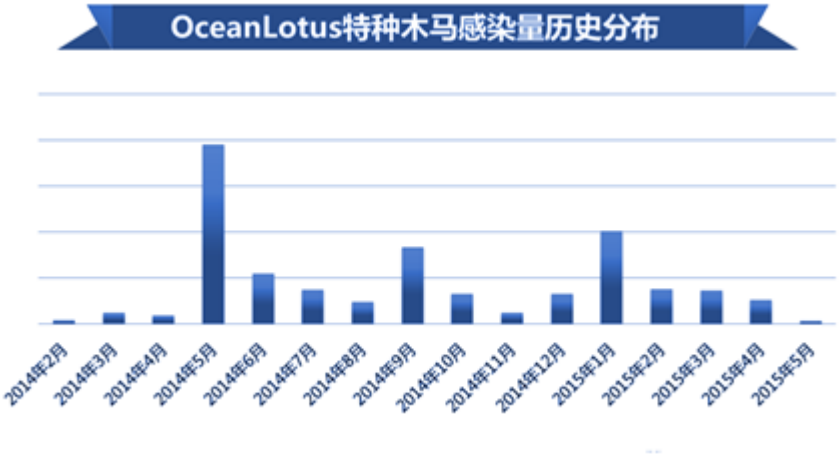
目前已经捕获的与OceanLotus相关的第一个特种木马出现在2012年4月。在此后的3年中，我们又先后捕获了与该组织相关的4种不同形态的特种木马程序样本100余个，这些木马的感染者遍布国内29个省级行政区和境外的36个国家。此外，为了隐蔽行踪，该组织还至少先后在6个国家注册了用于远程控制被感染者的C2（也称C&C，是Command and Control的缩写）服务器域名35个，相关服务器IP地址19个，服务器分布在全球13个以上的不同国家。

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：

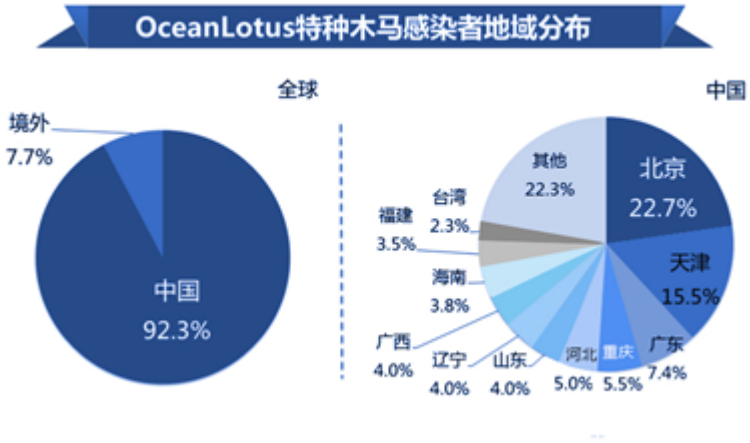
1）2012年4月，首次发现与该组织相关的木马。OceanLotus组织的渗透攻击就此开始。但在此后的两年左右时间里，OceanLotus并不活跃。
2）2014年2月，OceanLotus开始通过鱼叉攻击的方法对我们国内目标发起定向攻击，OceanLotus进入活跃期，并在此后的14个月内对我国多个目标发动了不间断的持续攻击。
3）2014年5月，OceanLotus对国内某权威海洋研究机构发动大规模鱼叉攻击，并形成了过去14个月中鱼叉攻击的最高峰。
4）同样是在2014年5月，OceanLotus还对国内某海洋建设机构的官方网站进行了篡改和挂马，形成了第一轮规模较大的水坑攻击。
5）2014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。

第二章 OceanLotus**攻击手法**

一、攻击手法概述

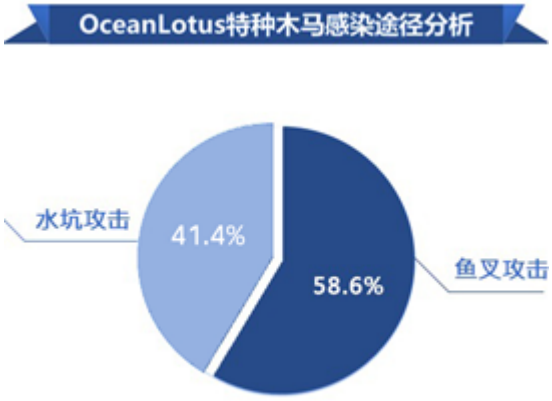
OceanLotus主要使用两类攻击手法:一类是鱼叉攻击，一类是水坑攻击。

鱼叉攻击（Spear Phishing）是针对特定组织的网络欺诈行为，目的是不通过授权访问机密数据，最常见的方法是将木马程序作为电子邮件的附件发送给特定的攻击目标，并诱使目标打开附件。

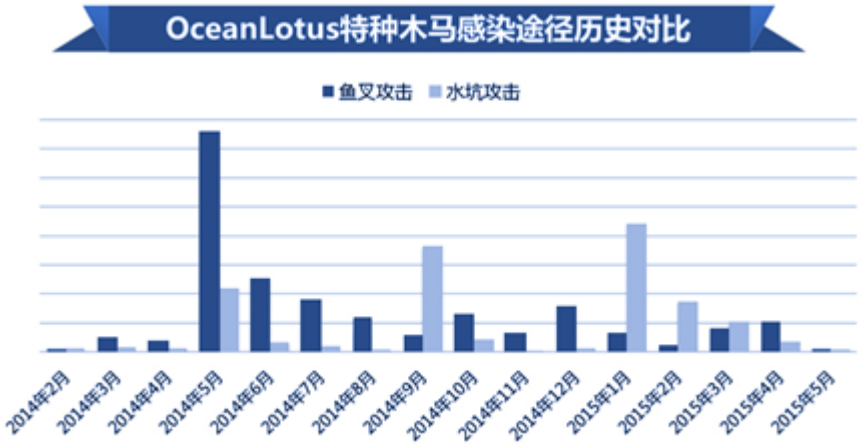
水坑攻击（Water Holing）是指黑客通过分析攻击目标的网络活动规律，寻找攻击目标经常访问的网站的弱点，先攻下该网站并植入攻击代码，等待攻击目标访问该网站时实施攻击。

下图给出了OceanLotus使用鱼叉攻击和水坑攻击的基本方法。

从目前受害者遭到攻击的情况看，鱼叉攻击占58.6%，水坑攻击占41.4%。



下图给出了因鱼叉攻击或水坑攻击而感染OceanLotus特种木马的电脑数量历史分布。从图中可以看出，鱼叉攻击的最高峰出现在2014年5月，而水坑攻击的最高峰出现在2015年1月。此外，2014年5月和2014年9月也是两个水坑攻击的高峰期。



鱼叉攻击

OceanLotus组织会非常有针对性地挑选目标机构，并收集目标机构人员的邮箱信息，再通过向这些邮箱中投递恶意邮件实现定向攻击。当受害者不小心点击执行邮件附件后，电脑就会感染OceanLotus特种木马，木马与C2服务器相连接后，用户系统由此就落入OceanLotus组织的控制网络中。监测显示，从2014年2月至今，OceanLotus的鱼叉攻击始终没有停止，每个月都有新的受害者增加。

在OceanLotus用于进行鱼叉攻击的邮件中（以下简称“鱼叉邮件”），附件通常是使用Microsoft Word程序图标的.exe可执行文件，为了提高攻击的成功率，攻击者通常会采用当前热点事件或关乎用户自身利益的话题为文件名，甚至有的文件名与所攻击的目标机构看起来有密切关联，形成非常显著的定向APT攻击的特征。以下是两个具体的例子：

1）新疆乌鲁木齐暴恐事件相关鱼叉邮件

2014年5月22日，中国新疆乌鲁木齐发生了暴恐事件。而5月28日，我们就捕获到了一个名为“最新新疆暴动照片与信.jpg.exe”的钓鱼文件通过电子邮箱进行发送。

2）公务员工资改革相关内容鱼叉邮件

2014年至2015年间，中国政府出台了《公务员工资改革新方案》，该方案直接影响政府机关从业人员。中国约有700多万公务员，公务员工资改革很长一段时间内，是政府机关人员舆论的热点话题。

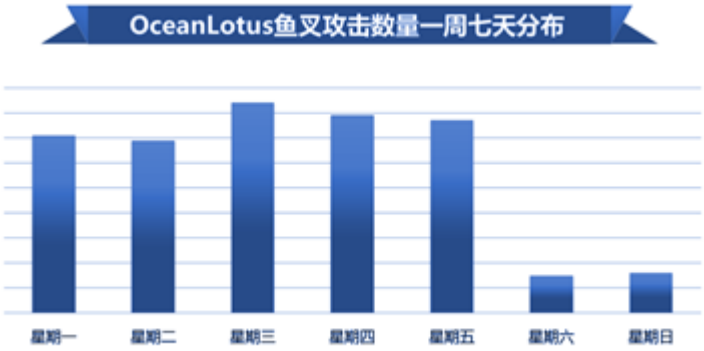
2014年9月9日，我们截获名为“工资制度以及特殊津贴.exe”的恶意邮件附件；2014年11月5日，我们又截获名为“工资待遇政策的通知.exe”的恶意邮件附件。在此期间，还有其他类似的恶意邮件附件被截获。而分析显示，这些邮件全部为OceanLotus组织向政府工作人员投递的鱼叉邮件。

通过不间断地对该组织的鱼叉邮件进行跟踪分析，据最近的统计数据显示，OceanLotus组织最常使用的附件存在一定的规律：邮件内容和附件的命名与海洋相关企事业机构建设、海洋资源、中国的党政机关、科研院所等密切关联，部分文件列表如下（有关机构名称及敏感内容用“*”代替）：

相关文件名
关于国家***研究中心工程建设的函.exe
国家**局的紧急通报.exe
最新新疆暴动照片与信息.jpg.exe
本周工作小结及下周工作计划.exe
厅关于印发《2014 年应急管理工作要点》的通知.exe
2015 年 1 月 12 日下发的紧急通知.exe
商量好的合同.exe
部关于开展 2015 年调查工作的通知.exe

一些特种木马的恶意样本之所以会使用很长的文件名，一个重要的原因是利用 Windows**的文件名显示机制使文件后缀**".exe"**不会自动被显示出来。所以，对于绝大多数文件接受者来说，即使电脑系统设置为显示文件后缀名，也很有可能因为文件名过长而使文件后缀名不能正常显示。**

统计还显示，OceanLotus发动的鱼叉攻击也具有很强的时间性和周期性。在一周7天中，工作日，即星期一至星期五截获的鱼叉攻击数量较多，而周末截获的鱼叉攻击数量则往往不及工作日的1/5。



水坑攻击

OceanLotus**组织在设置水坑时，主要采用两类方式：一是入侵与目标相关的**Web**应用系统，替换正常文件或引诱下载伪造的正常应用升级包，以实现在目标用户系统上执行恶意代码的目的；二是入侵与目标相关的**Web**应用系统后，篡改其中链接，使其指向**OceanLotus**设置的恶意网址，并在指向的恶意网址上设置木马下载链接。**

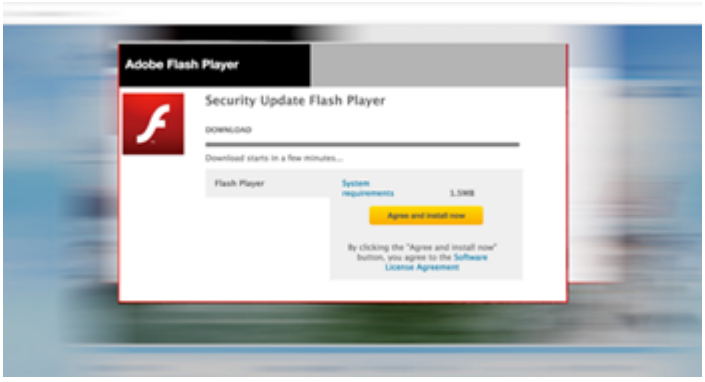
为了避免暴露，OceanLotus发动水坑攻击的持续周期一般很短，通常是在3-5天之内，几天之后攻击完成，OceanLotus就会将篡改的内容删除或恢复，将设置的水坑陷阱填平。因此，通常来说，想要事后复原水坑攻击的现场比较困难。

下面是通过技术手段恢复的两个OceanLotus组织设置的典型水坑案例。

1）水坑A

OceanLotus组织首先通过渗透入侵的攻击方式非法获得某机构的文档交流服务器的控制权，接着，在服务器后台对网站上的“即时通”和“证书驱动”两款软件的正常安装文件捆绑了自己的木马程序，之后，当有用户下载并安装即时通或证书驱动软件时，木马就有机会得到执行。攻击者还在被篡改的服务器页面中插入了恶意的脚本代码，用户访问网站时，会弹出提示更新Flash软件，但实际提供的是伪装成Flash升级包的恶意程序，用户如果不慎下载执行就会中招。

下图为用户访问该水坑站点时，攻击者的JS代码生成的提示用户下载执行伪造Flash升级包的页面。



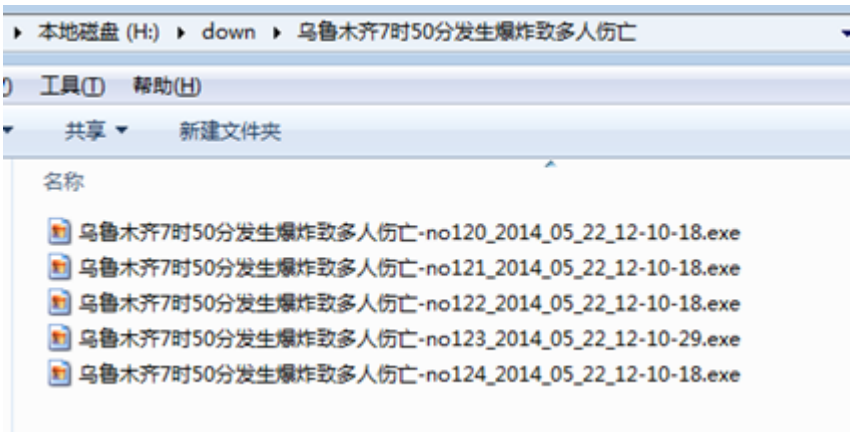
该组织的专业之处还体现在，水坑攻击会识别访问来源的操作系统平台，并根据客户端返回的系统信息，返回针对不同平台的恶意代码。在Windows平台下我们使用不同的浏览器访问该页面都会提示下载名为“install_flashplayer.exe”的更新文件；当操作系统为Mac OS时，水坑则向Safari浏览器推送能在MAC OS环境中运行的恶意更新程序“install_flashplayer_mac.zip”。

2）水坑B

被入侵的网站是一个政府站点，主要面向海洋相关研究类人员、专家提供文献下载、研究项目发稿和相关时事通告等功能。OceanLotus组织入侵网站以后修改了网站的程序，在用户访问公告信息时会被重定向到一个攻击者控制的网站，提示下载某个看起来是新闻的文件，比如在新疆522暴恐事件的第二天网站就提示和暴恐事件相关的新闻，并提供“乌鲁木齐7时50分发生爆炸致多人伤亡.rar”压缩包给用户下载，而该压缩包文件内含的就是OceanLotus组织的特种木马。

在该政府网站上，当用户点击某个通告链接时会提示文件下载，如下图：

提示框中的download.mail-attach.net为组织控制的服务器，将下载的“乌鲁木齐7时50分发生爆炸致多人伤亡.rar”压缩包文件解压后，可以看到文件夹内包含显示为JPG图片图标的exe可执行文件。若此时目标用户点击该文件，系统就会被感染。如下为部分下载回来的文件列表：



与此同时，在该服务器水坑文件同级目录下还发现存放了部分用于鱼叉攻击的恶意代码，证实了这起水坑攻击与之前提及的鱼叉攻击为同一组织发起。如下是部分文件列表：

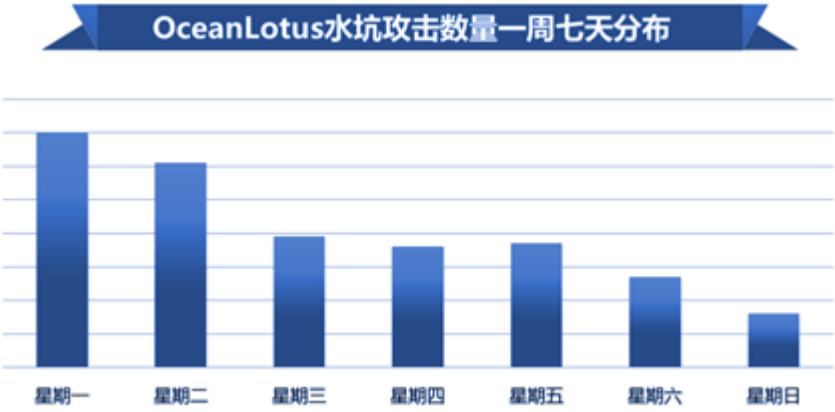
通过对该组织水坑式攻击手法的跟踪分析，发现该组织如果有机会入侵与目标相关的服务器，就会尽可能替换服务器上可能被下载的正常程序，诱骗用户下载并执行伪造的应用升级包。

下表为部分水坑服务器中出现的恶意文件：

文件名	文件 MD5
install_flashplayer.exe	7e68371ba3a988ff88e0fb54e2507f0d
rtx.exe	0529b1d393f405bc2b2b33709dd57153
sinopec.exe	9fea62c042a8eda1d3f5ae54bad1e959
报表插件安装程序.exe	486bb089b22998ec2560afa59008eafa
USBDeview.exe	b778d0de33b66ffdaaf76ba01e7c5b7b
DSC00229.exe	53e5718adf6f5feb2e3bb3396a229ba8
install_flashplayer13x37.exe	d39edc7922054a0f14a5b000a28e3329
NetcaEKeyClient.exe	41bced8c65c5822d43cadad7d1dc49fd

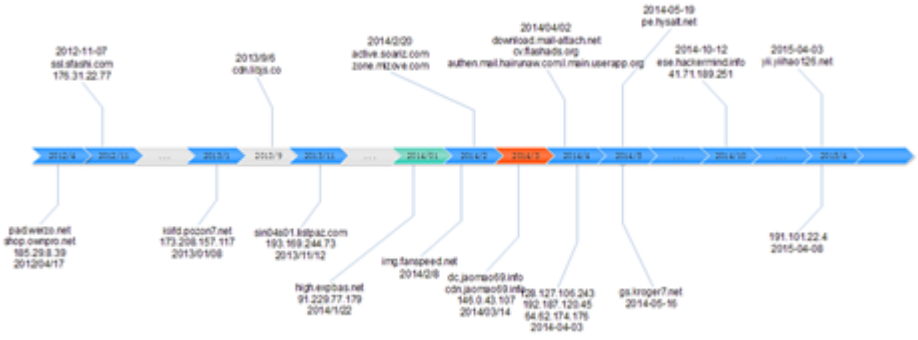
从目前截获OceanLotus发动的水坑攻击的情况来看，每周的周一和周二感染者数量最多。**分析认为，这可能是因为攻击者认真研究了政府和科研机构等工作人员的上网习惯。**由于水坑攻击容易将组织信息泄漏，因此，OceanLotus每发动一次水坑攻击的周期一般都不会超过3天。而如果要使3天的攻击

更加有效，就需要考虑攻击目标会在一周中的哪些天更容易访问水坑网站。由于中国政府和研究机构的工作人员往往有在星期一、二登录办公系统查询重大内部新闻和通知的习惯，所以在一周的前两天发动水坑攻击，效果相对更好。

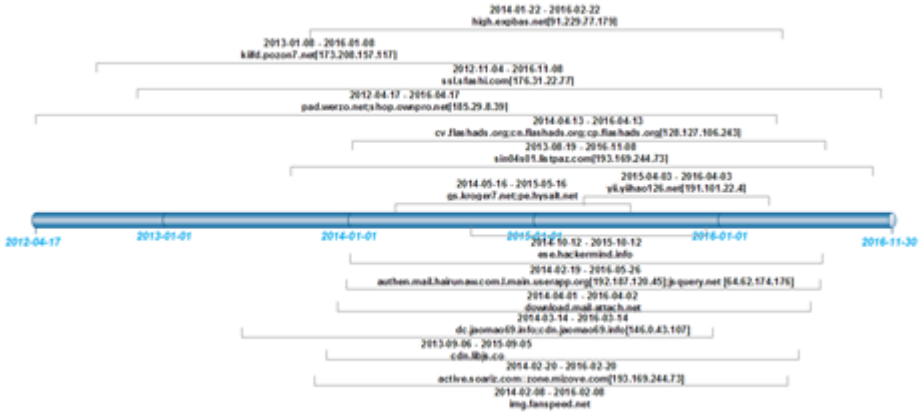


二、域名变换

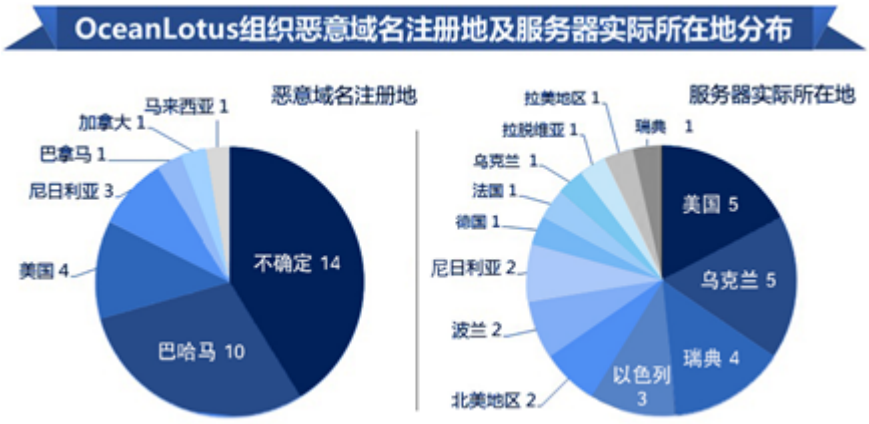
为了隐藏自己的真实身份，OceanLotus组织经常变换下载服务器和C2服务器的域名和IP。统计显示，在过去的3年中，该组织至少使用了C2服务器域名35个，相关服务器IP地址19个。而且大多数域名为了抵抗溯源都开启了Whois域名隐藏，使得分析人员很难知道恶意域名背后的注册者是谁。下图给出了OceanLotus注册各个域名时间点信息。



通过对攻击活动相关域名的统计，我们按注册时间的先后顺序对各个域名做了排序。时间线疏密程度显示该组织在2014年2月至2014年4月申请了大量的新域名。域名的生命周期如下图所示：



这些恶意域名的注册地和服务器也分布在世界各地。从注册地来看，最大的注册地是巴哈马10个，其次是美国4个，尼日利亚3个。从服务器实际所在地来看，美国和乌克兰最多，各5个，其次是瑞典4个，以色列3个。



按时间先后顺序排列，部分较活跃的域名详情如下：

域名	绑定 IP	注册时间	用途
pad.werzo.net	185.29.8.39	2012/4/17	C2，Mac OS
shop.ownpro.net	185.29.8.39	2012/4/17	C2，Mac OS
ssl.sfashi.com	176.31.22.77	2012/11/7	C2
kiifd.pozon7.net	173.208.157.117	2013/1/8	C2，Mac OS
cdn.libjs.co	62.113.238.135	2013/9/6	C2
sin04s01.listpaz.com	193.169.244.73	2013/11/12	C2
high.expbas.net	91.229.77.179	2014/1/22	C2
img.fanspeed.net		2014/2/8	C2
active.soariz.com	193.169.244.73	2014/2/20	C2
zone.mizove.com	193.169.244.73	2014/2/20	C2
dc.jaomao69.info	146.0.43.107	2014/3/14	Downloader
cdn.jaomao69.info	146.0.43.107	2014/3/14	C2
download.mail-attach.net		2014/4/2	Downloader
cnf.flashads.org	128.127.106.243	2014/4/3	钓鱼服务器
cn.flashads.org	128.127.106.243	2014/4/3	钓鱼服务器，Downloader，DNS
cv.flashads.org	128.127.106.243	2014/4/3	钓鱼服务器
cp.flashads.org	128.127.106.243	2014/4/3	钓鱼服务器
fpdownload.shockwave.flashads.org	128.127.106.243	2014/4/3	Downloader
authen.mail.haisunaw.com.1.main.userapp.org	192.187.120.45	2014/4/8	Downloader
jsquery.net	64.62.174.176	2014/4/8	C2
gs.kroger7.net	167.114.184.117	2014/5/16	C2
autoupdate.adobe.com			通过域名物种伪造的 Adobe 子域名，用于绕过安全检查措施。更新感染系统上的恶意程序

第三章 特种木马技术

从具体的攻击技术来看，OceanLotus先后使用过4种主要形态的特种木马，其中3种是Windows木马，一种是MAC系统木马。虽然这4种形态的木马均是以窃取感染目标电脑中的机密数据为目的的，但从攻击原理和攻击方式来看，却有着很大的区别。特别是针对Windows系统的3种特种木马形态，

其出现时间有先有后，危险程度不断升级，攻击方式从简单到复杂、从本地到云控，可以让我们清楚的看到该组织木马的技术发展脉络和攻击思路的不断转变。

根据这4种木马形态的攻击特点，我们将其分别命名为： OceanLotus Tester，OceanLotus Encryptor，OceanLotus Cloudrunner，OceanLotus MAC。

下面就针对OceanLotus特种木马的4种基本形态逐一进行技术分析。

1，OceanLotus Tester

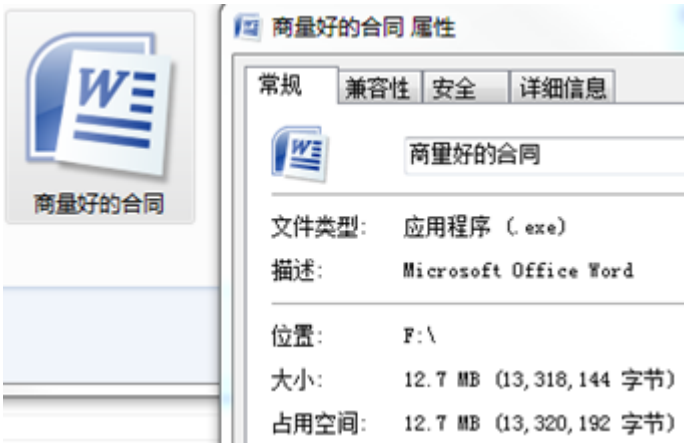
OceanLotus Tester最早被捕获于2012年，是一种比较简单的木马，与民用领域所见的一般间谍程序差别不大，安全软件也比较容易将其识别出来。从历史监测的数据来看，Tester的感染量微乎其微，在早期被捕获以后，长期处于不活跃的状态，在当时属于孤立出现的木马样本。

但是，在我们对OceanLotus特种木马的其他几个形态进行关联性分析时发现，早期出现的Tester木马在攻击对象、文件伪装特征、连接的C2服务器域名和窃取文件的特征等方面，与后来捕获的其他3种木马形态的样本存在诸多交集和共同点。我们因此判定，早期的Tester木马样本也属于OceanLotus这个组织所有。

我们猜测，Tester可能并不是OceanLotus组织正式使用的数字武器，很有可能仅仅是该组织成立初期，用以进行模拟攻击演练，以确定攻击体系可行性时所使用的一些测试代码。

2，OceanLotus Encryptor

Encryptor木马最早被截获于2014年2月。当时，安全人员截获了一批将自身图标伪装成Word文档或JPG文档的“.exe”文件，而且这些文件都还使用了一些颇具迷惑性的社工类文件名。下图就是Encryptor木马的某个样本伪装成文件名为“商量好的合同”的Word文档后，查看文件属性时的截图。其实仔细观看不难发现，文件的真实类型是应用程序（.exe）。



Encryptor木马的主要作用是打包和向C2服务器上传电脑中存在的各种Office文档，包括Word、PPT、Outlook邮箱文件等。而从攻击技术上来看，Encryptor木马最明显的特点就是会对自己的数据区进行随机递归加密处理，从而大大增加安全软件对其进行识别的难度。

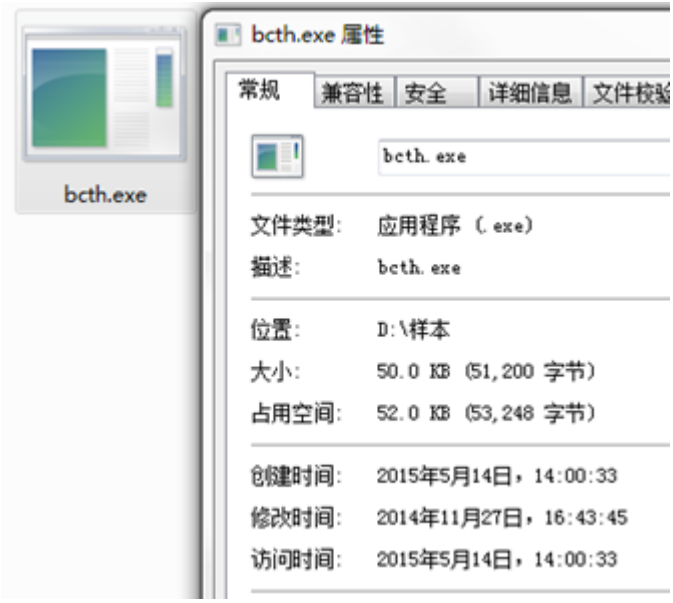
一旦有人下载并打开了Encryptor木马文件，这个木马就会通过以下一系列复杂的过程来进行自我释放。以伪装成Word文档的样本为例：

木马会首先释放出一个文件内容与文件名相符的Word文档，并在桌面上生成快捷方式，以迷惑受害者，接着解密释放出真正的木马程序，解密过程中使用了64位强密钥来绕过传统杀毒软件。木马一旦运行，就会自我删除释放代码的母体，因此很难捕获到这个木马的样本。

木马程序会用2种方法尝试加载名为Bundle.rdb的通信模块：自身加载或注入到一个系统进程，而Bundle.rdb木马模块一旦加载起来，就会和控制端通信完成C2通道的建立。这个程序也经过了一些精心的伪装。单独看其文件属性，稍不注意也会以为它就是QQ软件。整个木马的加载过程实际上就是一个木马与安全软件进行对抗的过程。不过，除了上述内容外，Encryptor还采用了填充垃圾数据的方法与安全软件进行对抗。例如用0×00或其他随机字符填充了十几M的文件内容，使得文件体积过大，从而避免样本被云系统上传。

3，OceanLotus Cloudrunner

Cloudrunner木马最早被截获于2014年11月。与之前的Encryptor木马不同，Cloudrunner木马只是一个体量很小的可执行文件，木马本身不显现任何恶意特征，在完成初始的感染以后，却会自动从指定的服务器上将其他木马程序下载到被感染的电脑上。这种攻击方式具有明显的云控特点。攻击者可以根据不同的需要，向被感染的电脑上发送各种不同的木马，从而使攻击更加隐蔽，也更具危险性。下图为查看该类木马文件的属性截图。



从木马特点上来看，此木马采用了 Shellcode**加密，解密执行，然后从网络下载接收第二阶段的木马功能模块，使木马在用户系统上的痕迹尽可能最小化，以逃避防恶意代码工具的查杀，并实现类似云控制的灵活性。**具体的信息收集及其他恶意操作以插件的方式投放到受感染的系统上并执行，功能包含如下表所列：

上传类别，	具体内容，
即时通信记录，	Yahoo、QQ、Skype等，
邮件数据，	ThunderBird、Foxmail、Mailease、MS Live、Outook，
文件信息，	安装程序、近期访问、驱动器目录，
系统信息，	账户、IP、共享、进程列表、网络连接，
屏幕监控，	，
网络流量监视，	，

4，OceanLotus MAC

OceanLotus MAC与OceanLotus Encryptor大致出现在同一时期，二者都属于OceanLotus使用的第二代木马程序。MAC木马主要针对Mac OS系统，主要作用是在水坑网站中诱骗用户下载执行。在APT攻击中，使用针对苹果操作系统的木马并不多见。

下面以某个样本为例来具体介绍MAC木马的攻击过程。

> 例子样本MD5：9831a7bfcf595351206a2ea5679fa65e

文件FlashUpdate.app\Contents\MacOS\EmptyApplication是一个Loader，

负责解密以下两个文件：

```
FlashUpdate.app\Contents\Resources\en.lproj\.en_icon
FlashUpdate.app\Contents\Resources\en.lproj\.DS_Stores
```

.en_icon相当于木马自身的副本，.DS_Stores是真正的执行体，解密并执行完这两个文件后,EmptyApplication会删除自身。

.DS_Stores程序会连接如下3个C2服务器域名： kiifd.pozon7.net， pad.werzo.net，shop.ownpro.net，并实现如下一系列的远程控制功能：

功能	命令
列目录	ls [path]
进入目录	cd [path]
获取当前目录	Pwd
删除文件	rm <file_path>
复制文件	cp <srcppath> <dstpath>
移动文件	mv <srcpath> <dstpath>
获取进程信息	p {info:pid | ppid | name}
杀掉进程	kill <pid>
执行命令	cmd <command system>
抓取通信	capture <saved_path>
显示文件	cat path [num_byte]
下载文件	download fromURLsavePath

MAC木马也具有较强对抗能力，具体包括以下几个方面：

> 1） 对其自身做了非常强的加密，分析时需要进行手工解密。
> 2） 木马会修改苹果浏览器的安全属性，使下载的程序直接运行而没有安全风险提示。
> 3） 木马会定时使用/bin/launchctl上传操作。
> 4） 木马会读取操作系统的版本。
> 5） 木马会检测Parallels虚拟机。

第四章 OceanLotus能力分析

通过对OceanLotus组织所使用的恶意代码、攻击载荷和诱饵数据的分析，该组织内部可能有多个小组，每个小组有自己的分工。组织中各组可能针对性地收集社工信息、开发定制的工具以及对窃取的情报进行集中二次处理挖掘，各个环节紧密配合，并在其内部共享窃取的情报信息和攻击载荷。概括来说，要达到目前已知的攻击效果，该组织至少应该具备如下能力：

> 1）精通目标国家的语言，跟踪相关的新闻时事；识别和分析需要进行攻击的目标人员，收集其相关的基本信息，确定攻击目标人员，设计针对性的攻击方式。
> 2）网络渗透和入侵能力，投递鱼叉邮件，设置水坑，抽取敏感数据，保持长期控制。
> 3）能够开发或者获取绕过当前主流防病毒工具的特种木马，持续改进和对抗。

对应到以上的3种能力，我们推测OceanLotus组织很可能存在3个小组，其基本能力及任务分工大致如下：

此外，考虑到OceanLotus组织制作的特种木马大多使用中文名称，而且往往紧贴中国国内最新时政变化，所以，该组织中一定有精通中文、了解中国国情的人专门从事有针对性的社会工程学研究。

第五章 OceanLotus攻击的捕获

随着“互联网+”时代的到来，越来越多的政府机构和企事业单位实现了网络化办公，并将内部的办公网络与外部的互联网相连。企业的互联网化在提高企业办公效率的同时，也使内部网络面临着越来越多的来自全球各地不同目的攻击者的网络攻击。

事实上，针对政府、机构和企业的APT攻击每天都在发生，甚至可以说，APT攻击就潜藏在我们每一个人的身边。OceanLotus也只不过是我们目前已经捕获到的数十起APT事件中的一个典型案例而已。

目前，已经有一些国际知名的安全企业，如FireEye、卡巴斯基等针对APT攻击展开了相关研究，并发布了相关的研究报告。而在国内，关于APT攻击的专业研究资料目前还非常有限。

造成这种状况的原因之一，是APT攻击具有很强的隐蔽性、针对性和对抗性特点，使用一般民用防御手段和木马查杀技术很难发现。针对APT攻击的捕获和检测技术也成为了近年来国内外安全公司和研究机构关注的焦点。

天眼实验室借助360公司多年在木马病毒、漏洞攻击的对抗过程中积累的经验，针对特种木马、0day/Nday漏洞攻击的检测和对抗等方面都进行了大量的探索和实践，使得运用这些特种木马或漏洞进行的APT攻击在我们的天眼系统中现形。

当然，除了针对特定的高级APT攻击过程的检测和防御外，目前捕获和研究APT攻击还面临着一个更大的挑战：如何将不同时间、不同地点、不同人群遭到的各种不同形式的网络攻击事件关联起来，形成一个APT攻击的全貌。目前国外关于APT攻击的研究也大多集中在对个别目标实体的、短周期攻击过程的研究上，很少有机构能够进行较大时间尺度和较大地域范围内的APT攻击研究。

OceanLotus所发动的APT攻击，攻击周期长达3年之久，攻击地域遍布国内29个省级行政区和境外的36个国家，鱼叉攻击、水坑攻击，前后不下几十个轮次，被黑网站也多达十几个。而且在这3年多里，OceanLotus还先后使用了至少4种不同程序形态、不同编码风格和不同攻击原理的木马程序，恶意服务器遍布全球13个国家，注册的已知域名多达35个。

因此，对于OceanLotus发动的这种范围大、时间长，但目的明确、目标精准的APT攻击，如果单独依靠传统的各种局部检测与防御技术，即便能够发现一些零星的攻击事件和病毒样本，也很难复原整个APT攻击的全貌。

天眼实验室此次捕获的OceanLotus组织及其攻击，主要使用了多维度大数据关联分析的方法。我们将百亿级的恶意程序样本库、数亿级的安全终端的防护数据、PB级的搜索引擎的全网抓取数据以及其他多个维度的互联网大数据进行了关联分析和历史检索，最终在每天海量的网络攻击事件中定位出与OceanLotus相关的各种攻击事件和攻击元素，最终绘制出OceanLotus组织对我国境内目标发动APT攻击的全貌。

目前，能够在实践中使用大数据方法分析定位APT攻击的研究机构并不多，同时，具有互联网大数据的处理与分析能力和高级攻防对抗经验的安全企业寥寥。天眼实验室针对未知威胁和APT攻击的研究是建立在360公司多年积累的安全大数据和互联网安全技术方法的基础之上的，因此能够捕获一些以往国内外其他研究者无法发现的威胁元素，并进行事件关联分析。我们也希望能够通过这种新的基于大数据的互联网安全研究成果，给其他网络安全工作者提供一些有益的参考和帮助。

*** 作者/360安全卫士（企业账号），转载请注明来自FreeBuf黑客与极客（FreeBuf.COM）**

Tags: 攻击 , 木马 , 组织 , 水坑 , 文件 , 鱼叉 , 目标 , 相关 , 服务器 , 特种 ,

为您推荐了相关的技术文章:

1. 定时炸弹 - MQ 代理中危险的序列化数据
2. 构造PPSX钓鱼文件 - Evi1cg's blog
3. 360安全报告-2017年上半年网络诈骗趋势研究报告
4. Rasp 技术介绍与实现
5. 会找漏洞的时光机: Pinpointing Vulnerabilities

原文链接： www.freebuf.com