海莲花团伙的活动新趋势

September 04, 2017 • 360天眼实验室

传送门

“海莲花”团伙再活动，微步在线做出最新动向分析

前言

前天友商发布了一个关于海莲花APT团伙的新活动报告，揭露了一些新发现的样本和基础设施，**本文提供一些360威胁情报中心视野内的信息来构成更大的拼图。**

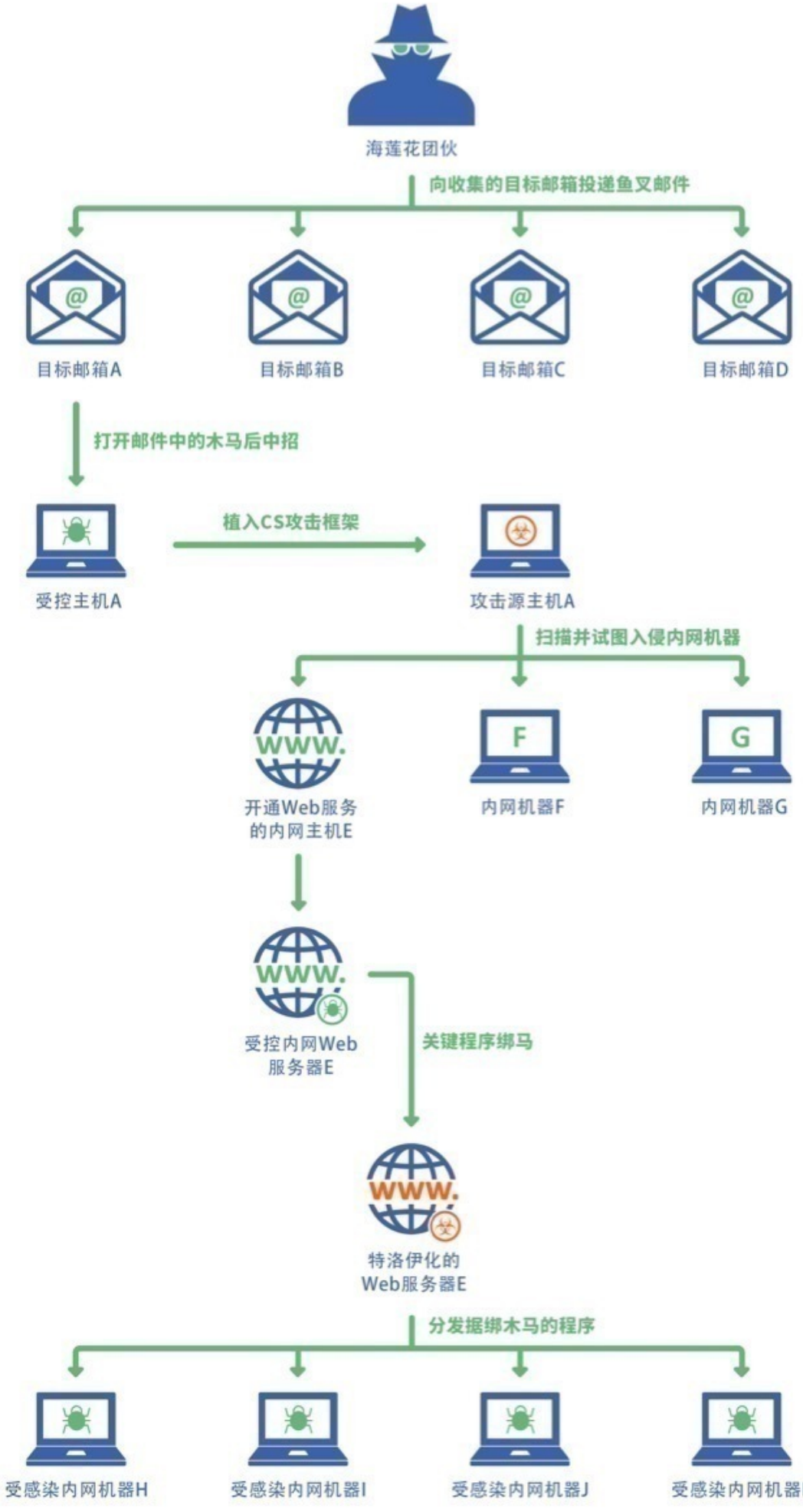
历史

自从2015年5月360威胁情报中心首次发布揭露海莲花APT团伙报告以来，我们一直持续关注着此团伙的活动，团伙只是在报告发布以后沉寂过一小段时间，此后从来就没停止过活动，力度甚至超过以

往。2016年6月，360威胁情报中心发布过又一篇跟踪分析：《海莲花重出水面》，介绍了结合终端和网络数据所监测到的更全面的攻击活动细节，详情可以参看链接：

https://ti.360.net/blog/articles/resurface-of-oceanlotus/

攻击活动可以简要以如下图来归纳：

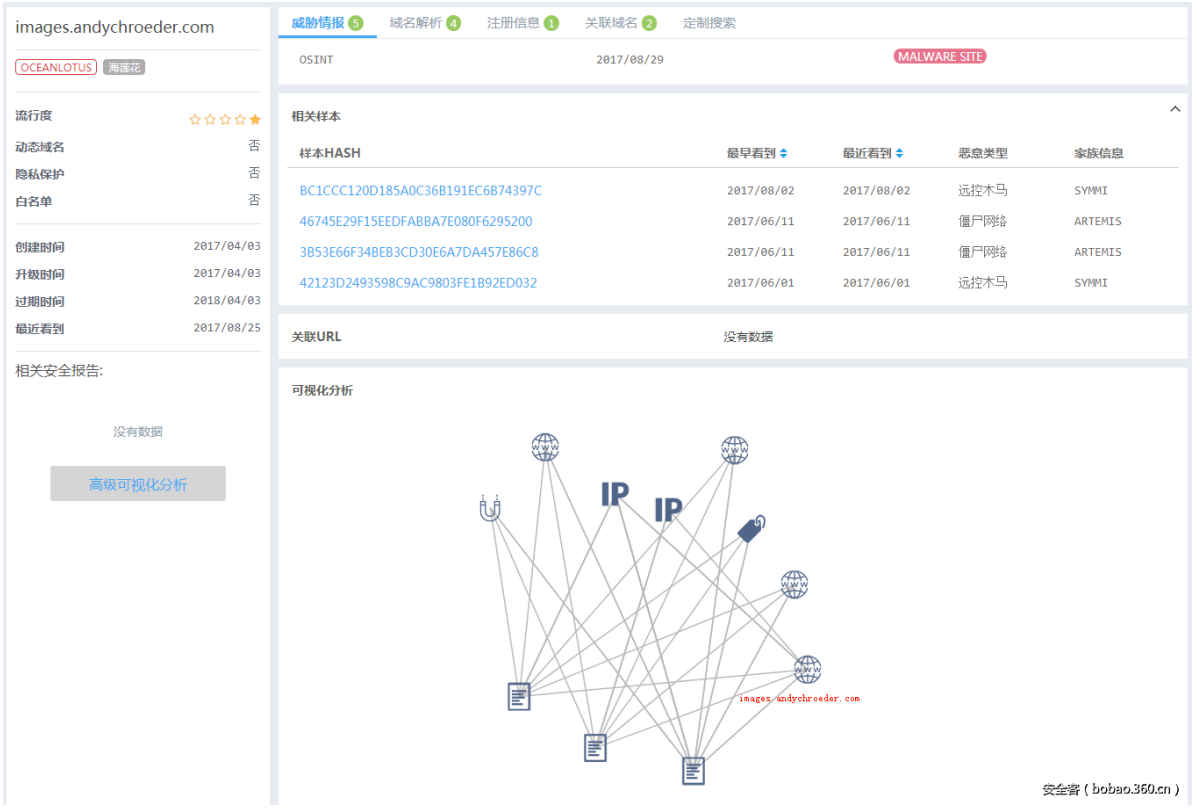


当时活动相关的TTP描述如下：

攻击阶段	特性描述
侦察跟踪	关注目标（主要是政府和海事相关）网站，尝试入侵，收集相关的电子邮箱
武器构建	使用多种现成的技术生成绑定木马诱饵程序，当前采用Powershell的Payload非常普遍
载荷投递	入侵网站构建水坑、发送定向鱼叉邮件
突防利用	利用似乎工作相关的内容进行社工诱导点击执行诱饵程序
安装植入	下载第二阶段Shellcode完成控制，以计划任务方式达成持久化
通信控制	之前使用自有实现的通信协议，当前较多地使用商业化攻击框架Cobalt Strike
达成目标	使用Cobalt Strike进行集成化的自动渗透，不太在乎隐秘性，只要有可能进一步创建更多水坑

现状

2017年7月360威胁情报中心截获并分析了多个海莲花团伙的新样本及对应的通信基础设施，相关的信息在威胁情报中心的数据平台上可以看到并且已经推送到天眼未知威胁检测系统及NGSOC的新版本中，用户如果查询到相关的IOC元素则可以立即看到平台输出的标签信息。



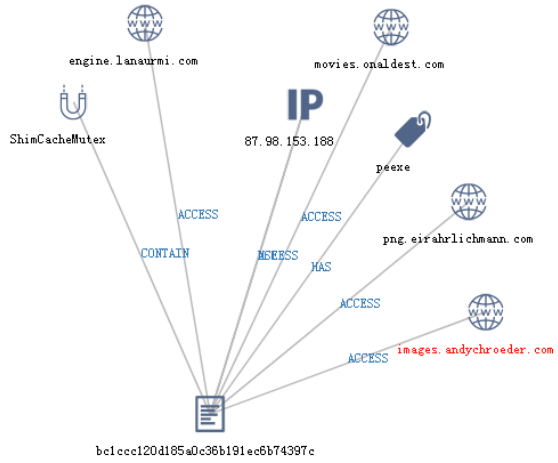
威胁情报中心发现的相关多个样本和IP/域名等基础设施：

相关样本

样本HASH	最早看到	最近看到	恶意类型	家族信息
BC1CCC120D185A0C36B191EC6B74397C	2017/08/02	2017/08/02	远控木马	SYMMI
46745E29F15EEDFABBA7E080F6295200	2017/06/11	2017/06/11	僵尸网络	ARTEMIS
3B53E66F34BEB3CD30E6A7DA457E86C8	2017/06/11	2017/06/11	僵尸网络	ARTEMIS
42123D2493598C9AC9803FE1B92ED032	2017/06/01	2017/06/01	远控木马	SYMMI

关联URL　　没有数据

可视化分析



安全客 (bobao.360.cn)

网络层的IOC方面主要涉及如下几个在2017年4月3日集中注册的域名（同天注册似乎是海莲花团伙的操作惯例，甚至可以作为识别团伙的特征之一）。

当前注册信息

创建时间	2017-04-03 07:02:24
过期时间	2018-04-03 07:02:24
更新时间	2017-04-03 07:37:05
注册人	Domain Admin
注册人所属组织	Whois Privacy Corp （ 相关域名150个 ）
管理员邮箱	andychroeder.com-admin-sign@customers.whoisprivacycorp.com （ 相关域名0个 ）
管理员电话	+1.5163872248
管理员传真	
国家代码	BS
域名服务商	Internet Domain Service BS Corp
域名服务器	ali.ns.cloudflare.com , mario.ns.cloudflare.com

安全客 (bobao.360.cn)

域名为：

```
engine.lanaurmi.com
movies.onaldest.com
images.andychroeder.com
png.eirahrlichmann.com
```

基于样本及其他数据源的得到的其他类型IOC见IOC节，相关的技术分析可能会输出单独的报告。

变化

基于对样本及更多其他来源数据的整合分析和历史活动的长期跟踪，我们发现海莲花团伙活动的一些变化，值得在此分享给安全社区：

1. **攻击所使用的木马后门工具更复杂对抗更强。**360威胁情报中心分析了若干个除Cobalt Strike组件以外的自研木马代码，发现其更加普遍地采用了白程序利用结合Shellcode的方式来绕过防病毒系统的检测，为了对抗人工分析恶意代码做了深度混淆。这个变化体现了团伙在技术能力上有了进一步地提升，使我们的分析工作需要更先进的工具，投入更多人力。

2. **与去年相比，海莲花团伙的攻击活动面有所收窄，但攻击目标的针对性加强，鱼叉邮件的社工特性突出，体现对攻击目标的深度了解。**有用户反馈到威胁情报中心的样本使用了如下的附件名：

```
invitation letter-zhejiang ***** working group.doc
```

星号是非常具体的目标所在组织的简称，目标人物在浙江省，所以附件名里加了zhejiang字样，暗示这是完全对目标定制的Payload。这与2016年采用的广撒网式的策略完全不同，体现了攻击目标的专注度。

3. **攻击所采用的网络基础设施做了更彻底的隔离，使之更不容易做关联溯源分析。**基于以往活动的分析，360威胁情报中心了解团伙所使用的IP偏爱193.169.*.*网段，过往很多攻击活动可以基于此非常容易地关联起来。今年的新近样本使用的网络基础设施与既往的没有重叠，非常"干净"。以往基于网络资源重叠的关联分析不再有效，导致分析人员需要耗费大量的人力去啃对抗加强后的样本以获取关联点，这些制造的麻烦虽然不至于使关联工作最终搁浅，但确实大大增加了资源的消耗。

4. **对之前已经攻击过的目标会进行反复攻击，发送新版本的鱼叉邮件尝试再次获取控制。**我们处理用户反馈的过程中发现对于海莲花团伙所认定的高价值用户，系统上的恶意代码由于被揭露而清除以后，攻击团伙还会尝试用新Payload进行攻击，对于之前已经控制的目标也会以新Payload转换控制所用的网络基础设施。

以上这些变化可以简单总结为海莲花团伙的技术水平在提升，与此同时攻击更加专注也更注意隐藏自己。

IOC

域名	说明
engine.lanaurmi.com	C&C
movies.onaldest.com	C&C
images.andychroeder.com	C&C
png.eirahrlichmann.com	C&C
store.shoesadidas.net	C&C
URL	
http://store.shoesadidas.net:80/newmodel.png	目前还处于活动状态
文件 HASH	
bc1ccc120d185a0c36b191ec6b74397c	GoogleUpdateSetup.exe
42123d2493598c9ac9803fe1b92ed032	Google Update Setup
3b53e66f34beb3cd30e6a7da457e86c8	KoreanTimesSSK.ttf
3bd041ef488806c55fbc40b4af24eabb	
46745e29f15eedfabba7e080f6295200	
d1e614479fee318904442c16c5ef4877	hgfs.dll
1f8ade068ba6fbfe8605e0946bf2d79f	ep7res01.dll
c117ea93410ad849e7a3ff9293bcd9ab	hp6000.dll 安全客（bobao.360.cn）

传送门

“海莲花”团伙再活动，微步在线做出最新动向分析

Tags: 团伙 ， 攻击 ， 分析 ， 活动 ， 威胁 ， 情报中心 ， 目标 ， 莲花 ， 样本 ， 发现 ，

为您推荐了相关的技术文章:

1. unserialize() 实战之 vBulletin 5.x.x 远程代码执行
2. Kaggle初探--房价预测案例之数据分析
3. 一篇文章走进Mac逆向的世界
4. S2-017重现过程
5. 通过Netflow进行攻击AS溯源

原文链接： www.anquanke.com