九维团队-暗队（情报）| “海莲花”APT近期攻击样本分析报告

原创 九维团队-暗队 安恒信息安全服务 2022-10-17 16:27 发表于北京

0、背景

“海莲花”（OceanLotus）又名OceanLotus Group、Ocean Lotus、Cobalt Kitty、APT-C-00、SeaLotus、Sea Lotus、APT-32、APT 32、Ocean Buffalo、POND LOACH、TIN WOODLAWN、BISMUTH等称号，是一个被网络安全业行业认为是据有越南政府背景的国家级APT组织。由天眼实验室于2015年首次披露，在首次披露的攻击活动中，其攻击目标涵盖了中国政府、科研院所、海事机构、海域建设、航运企业以及全球36个国家等。

“海莲花”针对东南亚私营公司的攻击行动至少从2014年开始，海莲花以在越南制造业、消费品和酒店业开展运营的外国公司为目标。

攻击行动概述：

· 2014年，一家欧洲公司在越南建设制造工厂之前遭到入侵。
· 2016年，越南和在网络安全、技术基础设施、银行和媒体行业工作的外资企业成为攻击目标。
· 2016年年中，在一家计划将业务扩展到越南的全球酒店业开发商的网络上检测到海莲花独有的恶意软件。
· 从2016年到2017年，位于越南境内的美国和菲律宾消费品公司的两家子公司成为海莲花入侵行动的目标。
· ……

“海莲花”针对外国政府以及越南持不同政见者和记者的攻击行动

除了重点针对与越南有联系的私营公司外，至少从2013年以来，海莲花还针对外国政府以及越南持不同政见者和记者。以下是该活动的概述：

· 电子前沿基金会发布的博客（原文链接：https://www.eff.org/deeplinks/2014/01/vietnamese-malware-gets-personal）指出，记者、活动家、持不同政见者和博客作者在2013年成为海莲花的目标。
· 2014年，海莲花利用一个名为“Plans to crackdown on protesters at the Embassy of Vietnam.exe”的鱼叉式钓鱼附件，针对东南亚越南侨民中的持不同政见者活动。同样在2014年，海莲花对一个西方国家的立法机构进行了一次入侵。
· 2015年，天眼发布了一份报告，海莲花以中国政府、科研院所、海事机构、海域建设和航运企业为目标。
· 2015年和2016年，两家越南媒体成为海莲花的攻击目标。
· 2017年，海莲花使用的诱饵中的社会工程内容提供了证据，证明它们可能被用来针对在澳大利亚的越南侨民成员以及在菲律宾的政府雇员。
· ……

一、概述

近日，安恒信息分子实验室反APT小组（九维团队-暗队）在日常的威胁狩猎中捕获到了“海莲花”的攻击活动样本。当用户打开WINWORD.EXE时，会加载恶意文件（MSVCR100.dll），该恶意文件会释放3个文件，分别执行持久化、下载下一阶段后门和信息收集并回传，该样本采用白+黑的方式实现防御规避，通过创建计划任务实现持久化。

小组通过对样本进行逆向分析，根据样本行为特征、C2以及结合开源情报，发现此次攻击活动背后的组织为“海莲花”APT。

二、样本分析

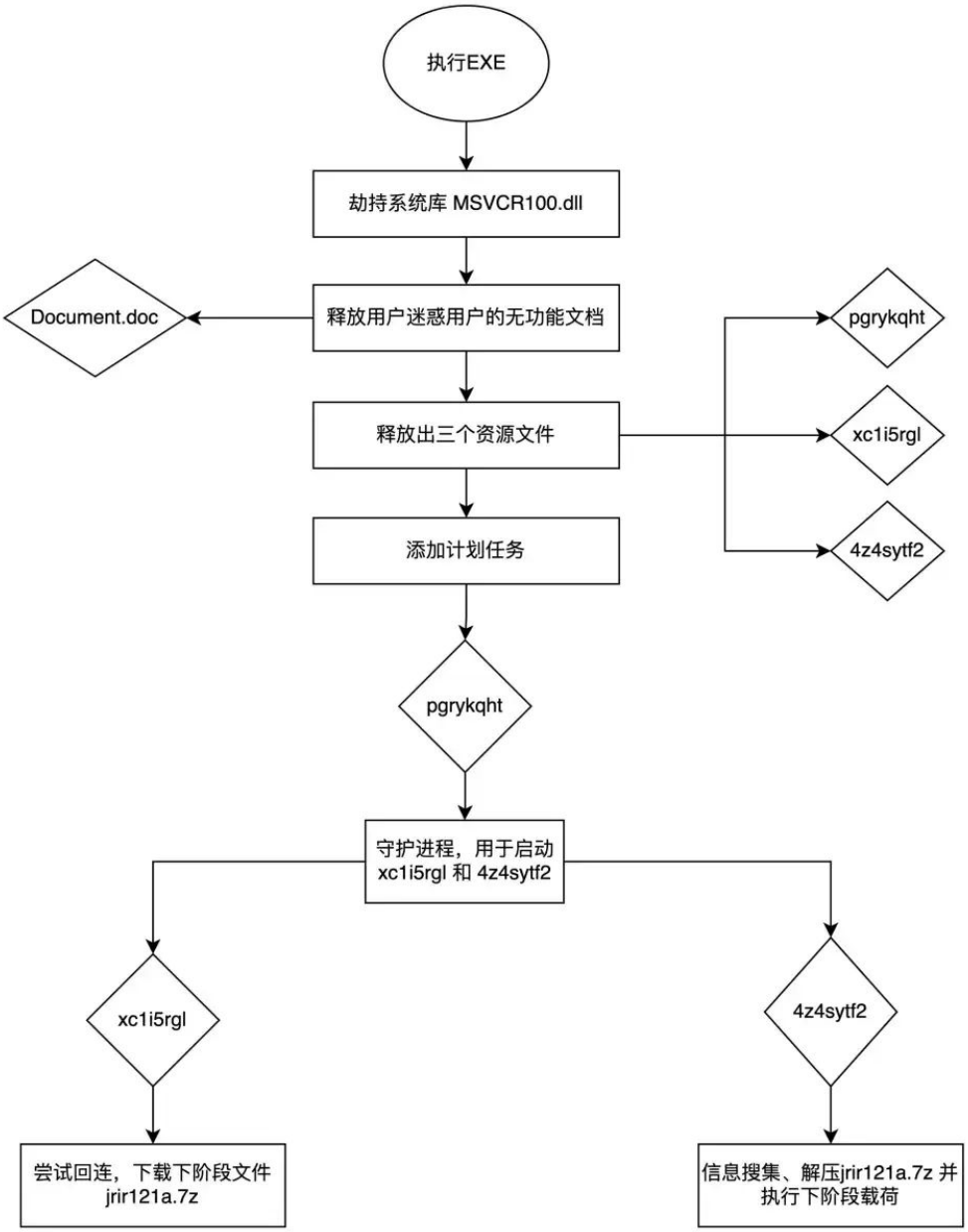
1、样本基础信息

说明：本次样本采用白+黑方式，白文件为 Office WINWORD.EXE

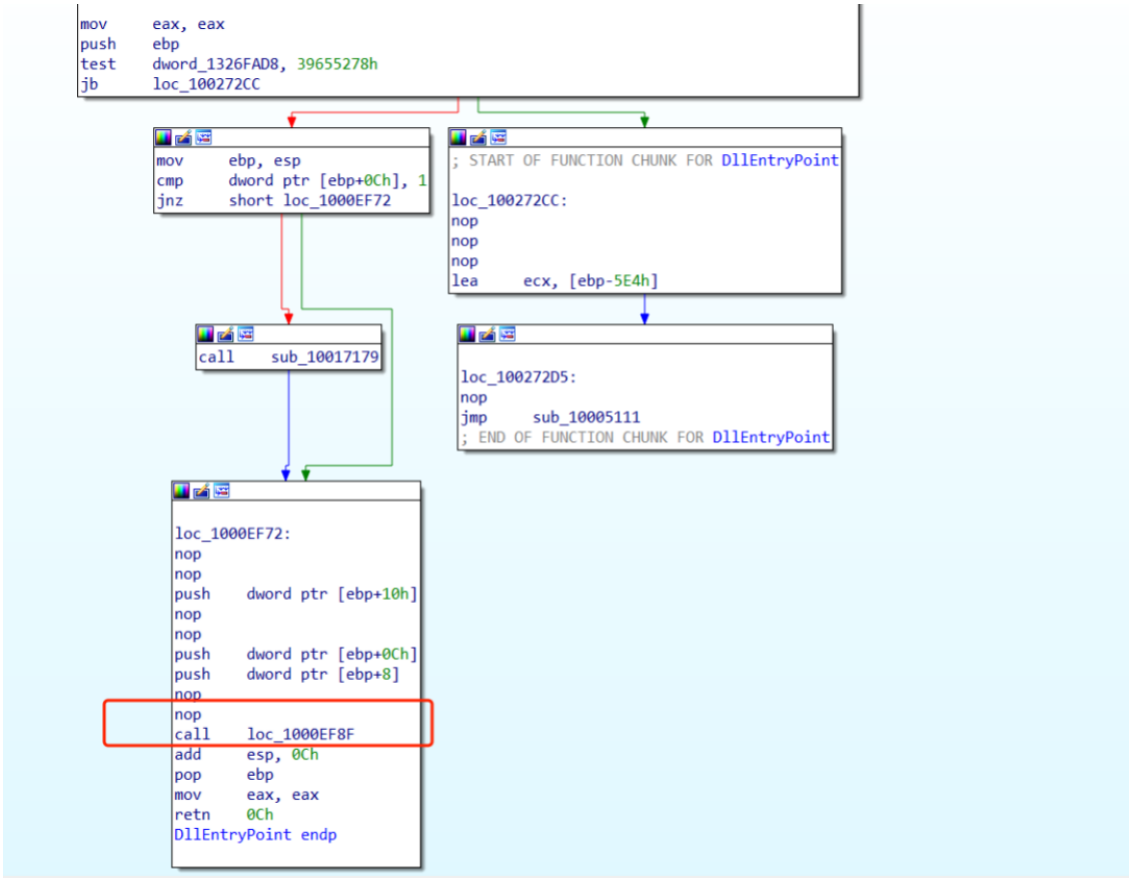
黑文件名: MSVCR100.dll
SHA256:46eecbbb37a99c735403c17141b21423e39032c53812b8a70446f43aa3ed0a0a
SHA1:a68b043e78fdf43a6e4946e463f980ce4f5febc9
MD5:1e8d4fbebbad2fe99857949146cf72de
编译时间： Wed Dec 20 21:17:37 2017

白文件名：Screenshot 2022-08-10 102463453453123213132534535478772115 1 - Microsoft Office 365 Online.exe
SHA256:3D46E95284F93BBB76B3B7E1BF0E1B2D51E8A9411C2B6E649112F22F92DE63C2
SHA1:81852cb9950604eda0918f625c71b0962865db23
MD5:7c22121f33af2bad8656ac09300416ee
编译时间: Sun Sep 30 01:49:14 2012

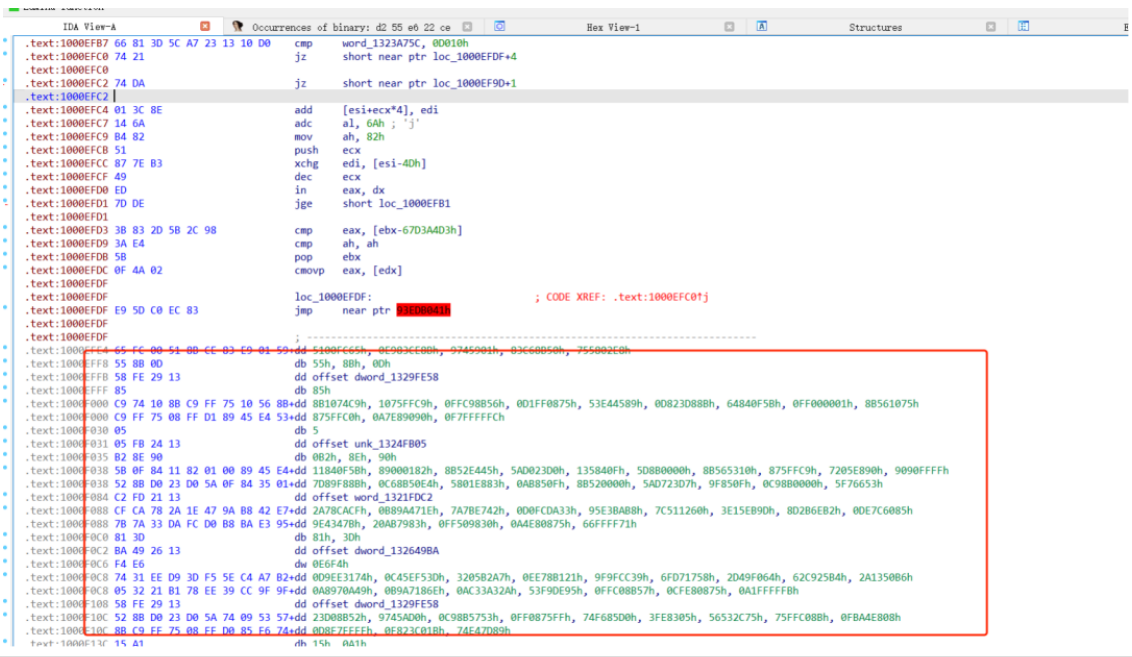
2、执行流程图


执行EXE
劫持系统库 MSVCR100.dll
Document.doc
释放用户迷惑用户的无功能文档
pgrykqht
释放出三个资源文件
xc1i5rgl
添加计划任务
4z4sytf2
pgrykqht
守护进程，用于启动
xc1i5rgl 和 4z4sytf2
xc1i5rgl
4z4sytf2
尝试回连，下载下阶段文件
jrir121a.7z
信息搜集、解压jrir121a.7z 并
执行下阶段载荷

入口：

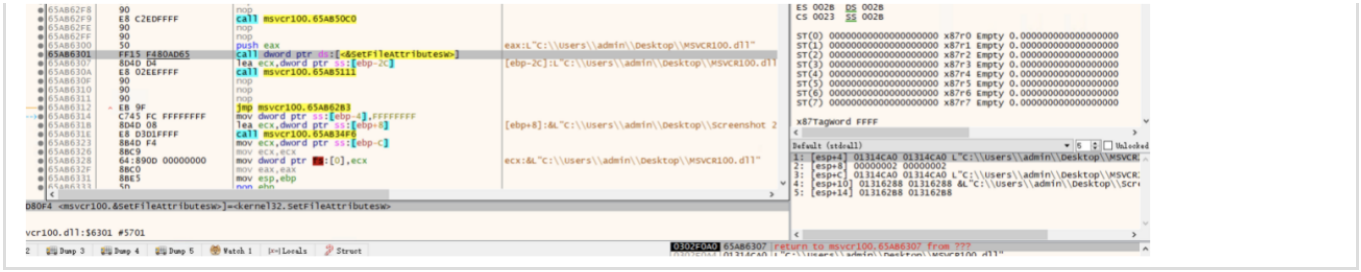


样本通过不透明谓词、花指令等方案对抗静态分析。



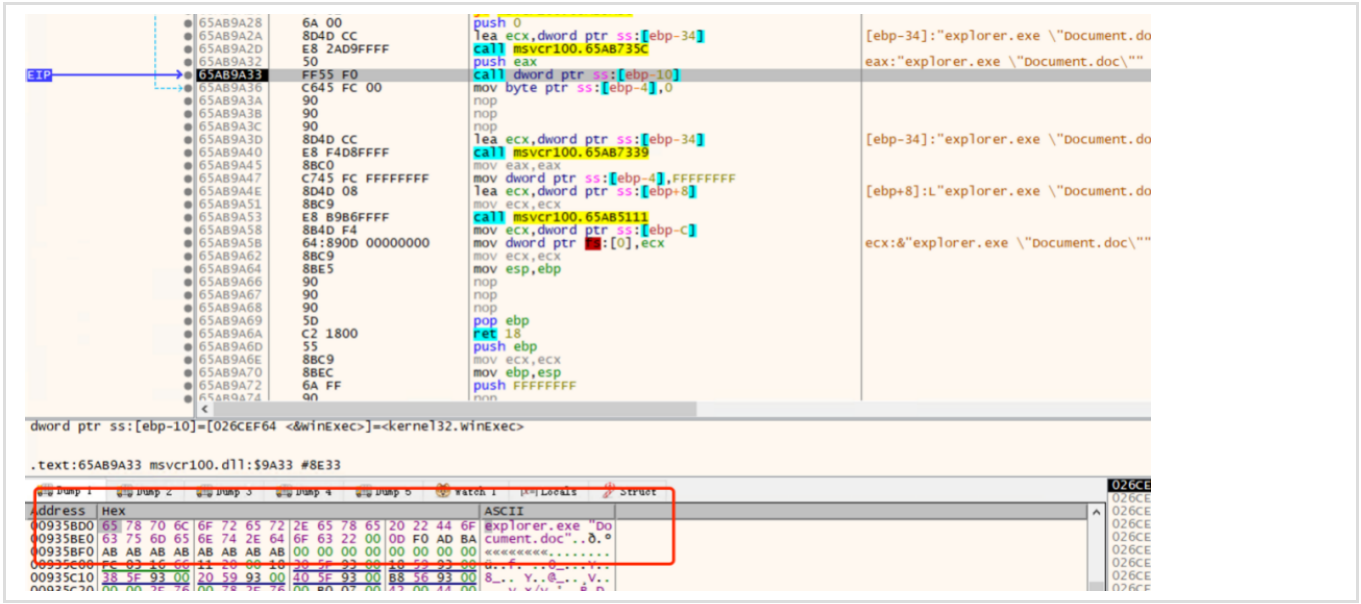
3、隐藏自身、打开迷惑文档

将主进程和DLL文件属性设置为隐藏。

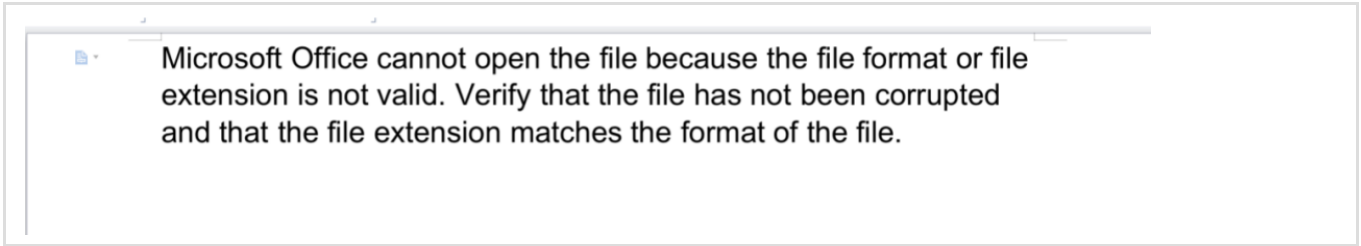


创建并写入文档文件 Document.doc 。

使用默认应用打开文档。

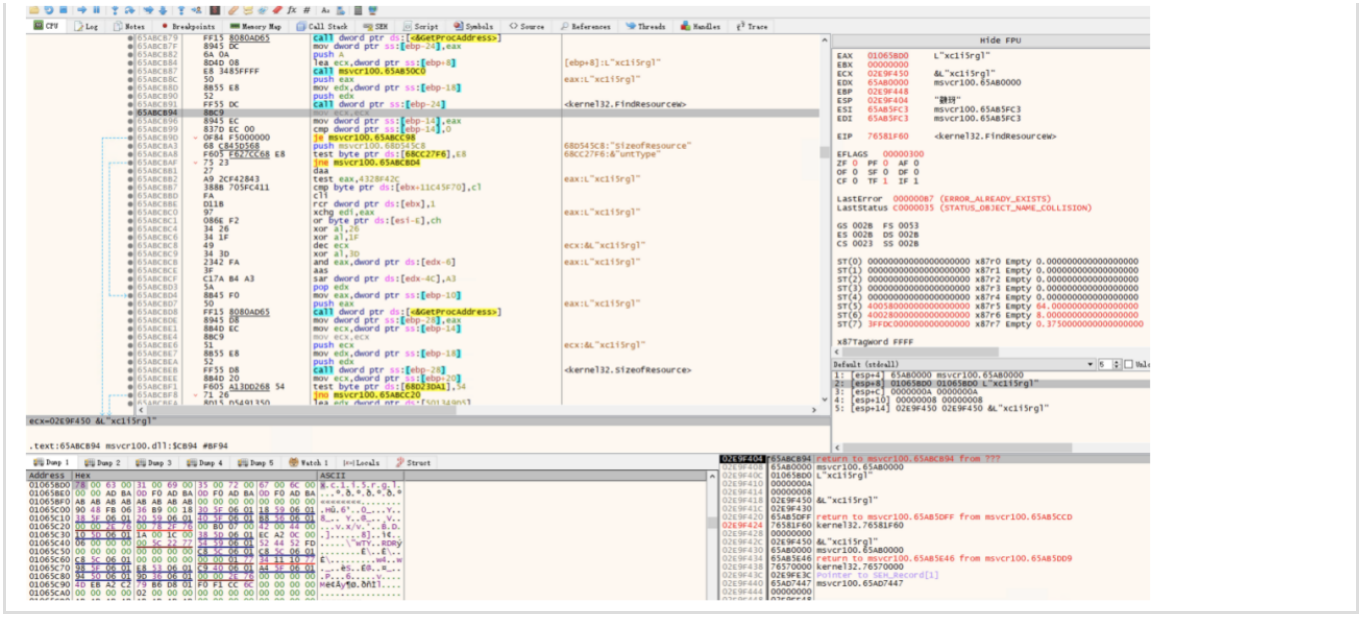


内容为特意制作的报错文档。

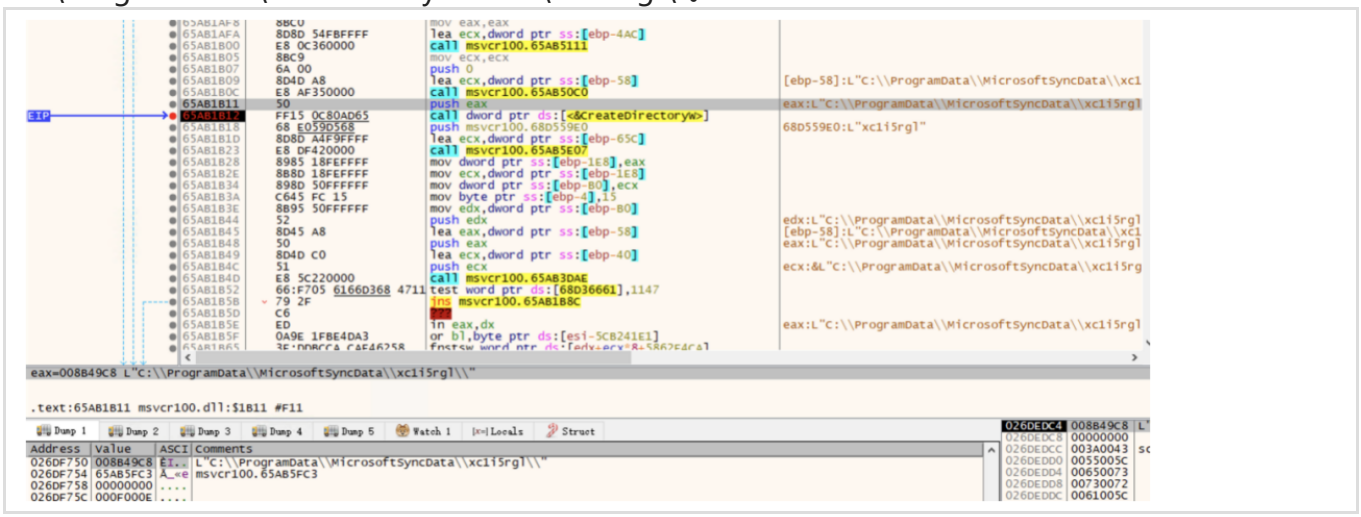


4、释放资源文件

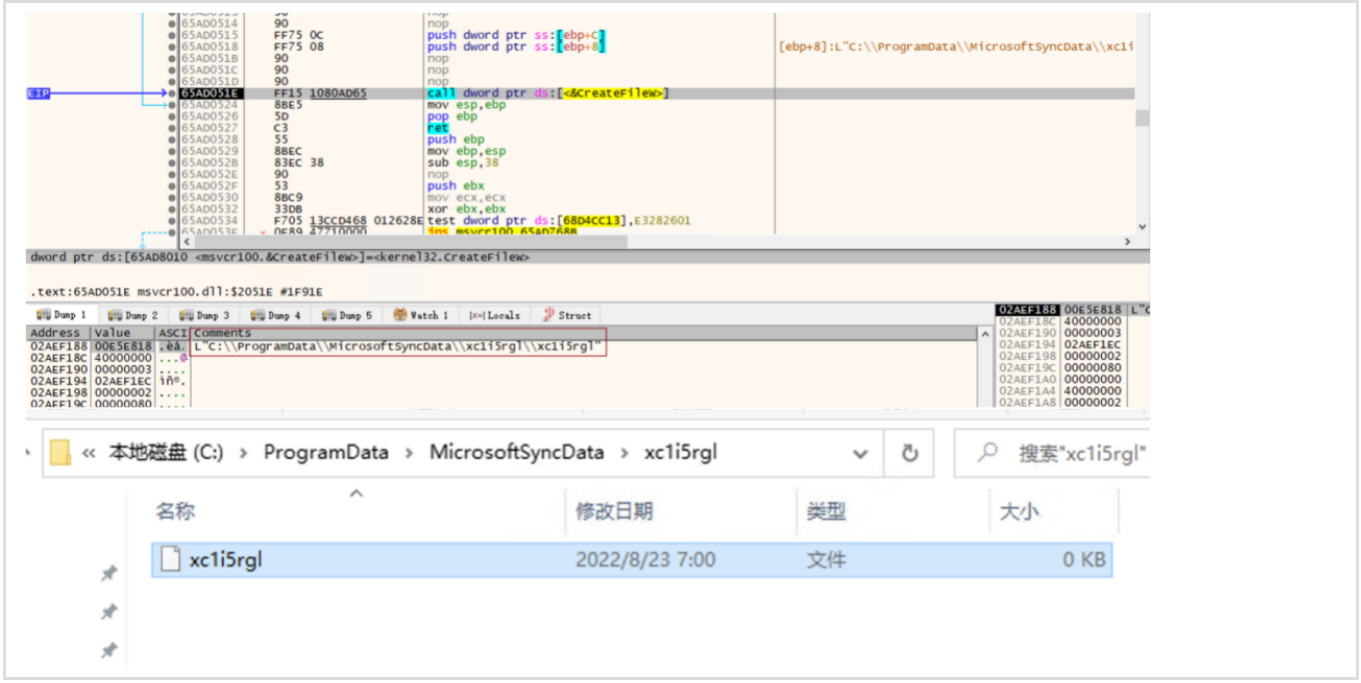
从资源区中提取内容。



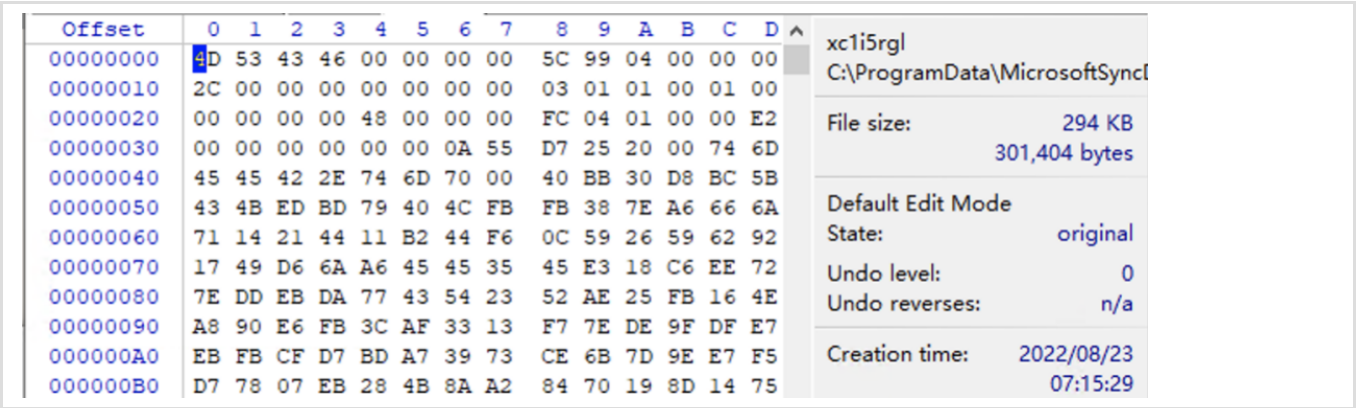
创建资源文件同名目录
“C:\ProgramData\MicrosoftSyncData\xc1i5rgl\”。



创建文件并写入文件。

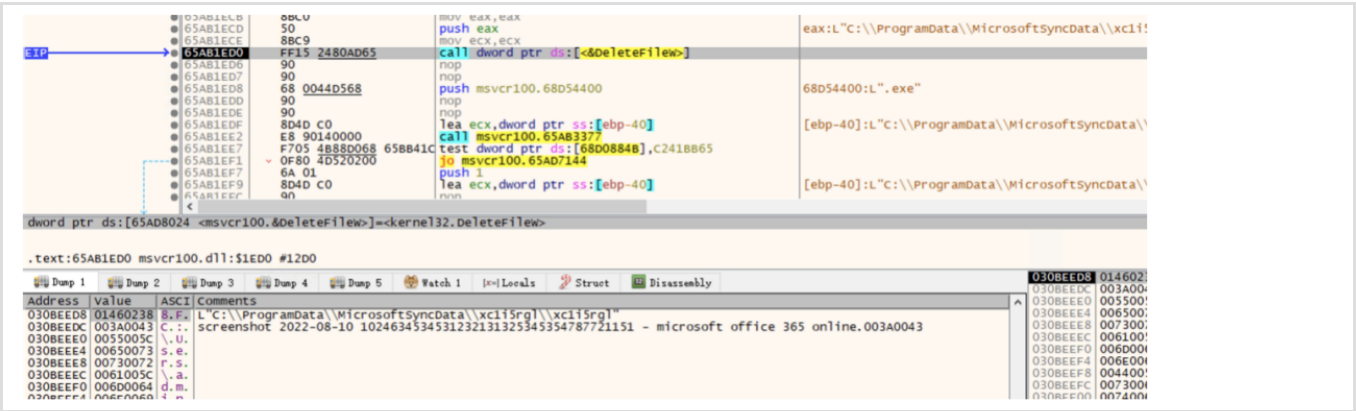


释放的文件为cab格式文件。

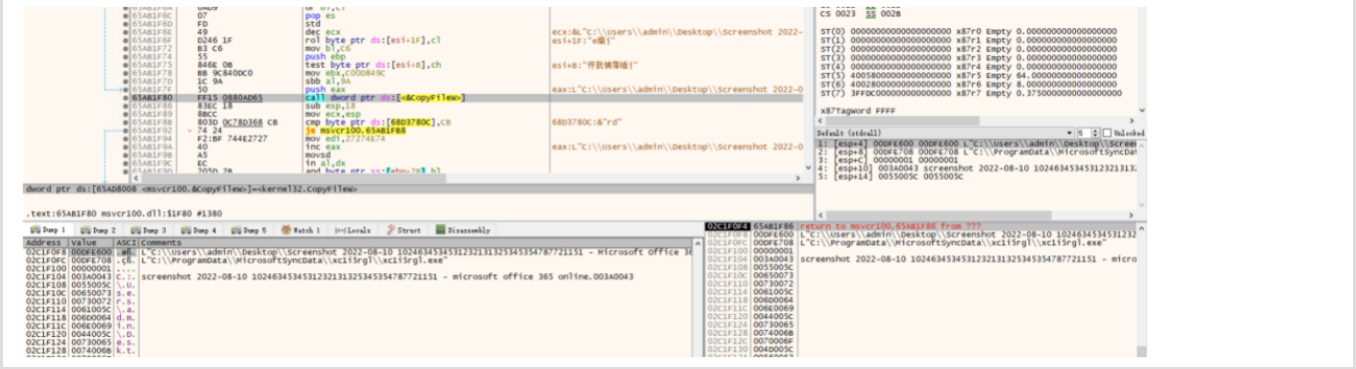


调用extrac32 解压 cab压缩文件，释放文件名为 MSVCR100.dll。

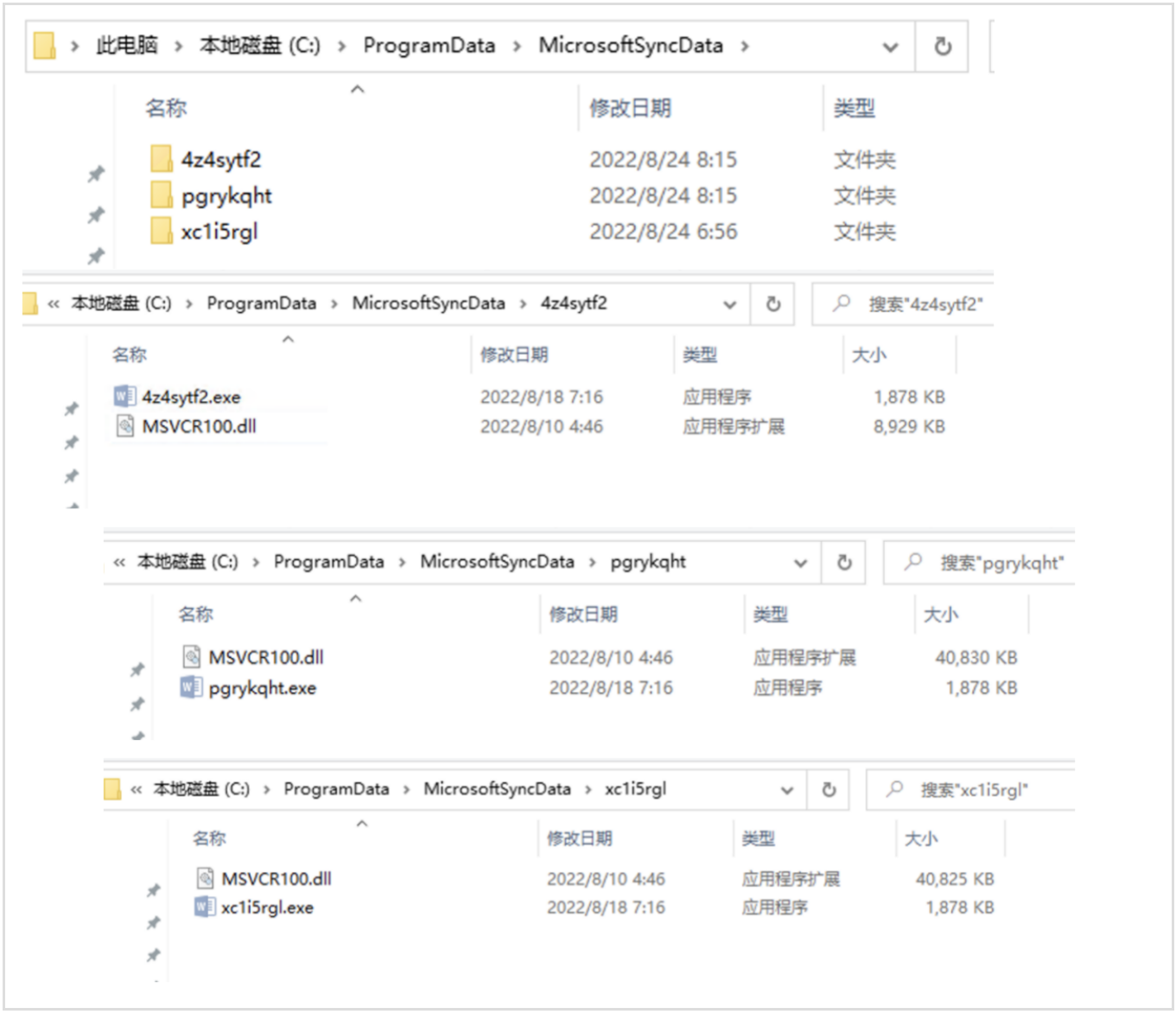
解压完成后，删除cab压缩文件。



拷贝主进程到该目录下：
C:\ProgramData\MicrosoftSyncData\xc1i5rgl



通过以上方法释放其他两个资源文件。



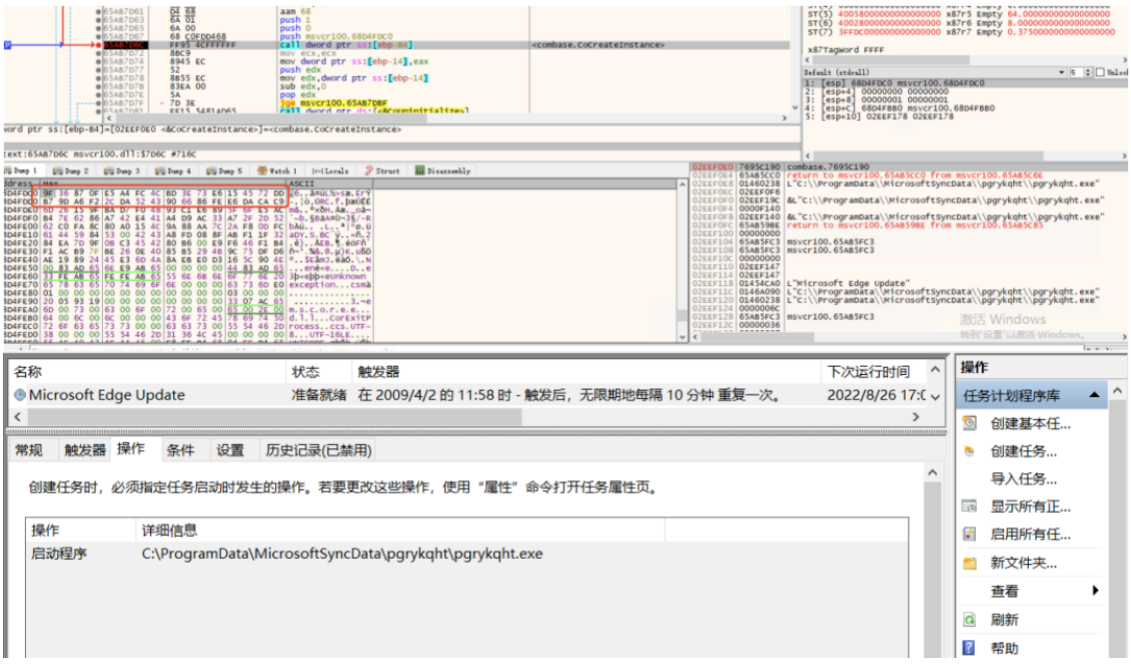
路径:
C:\ProgramData\MicrosoftSyncData\xc1i5rgl\MSVCR100.dll
SHA256:8DECBFC3B7B7238A80BE38407D8F65A96C1E4D4DEB9B1AC701C81675D5402A51
SHA-1:
38e63cf01869adc7251353f5552dc4dbaa271121
MD5:edf011dc7e9bd2c265cedb9ac5db7396
编译时间: Fri Aug 05 04:33:19 2016(MSVCR100.dll)

路径:
C:\ProgramData\MicrosoftSyncData\4z4sytf2\MSVCR100.dll
SHA256:1C920E2B0409DF1359827658CF0FCEA656A17FE11DB72A5E64B58425CAED2718
SHA1:6f18a31ccde5d3d30fa586e8c106644a0f984bf2
MD5:221c16803827861427454229296ce28c
编译时间:
Sat Sep 06 17:51:49 2014(MSVCR100.dll)

路径:
C:\ProgramData\MicrosoftSyncData\pgrykqht\MSVCR100.dll
SHA256:E64587C6DDF98B1B5DAC54C2A5BAD965740AC76F153702E92D6B2F7578C5C522
SHA1:dd15d4e0066a2b5e848e9b0ba48535fcec6a5169
MD5:d34ef9ae564aff98ed67846f2795f762
编译时间:
Fri Apr 16 20:44:02 2021(MSVCR100.dll)

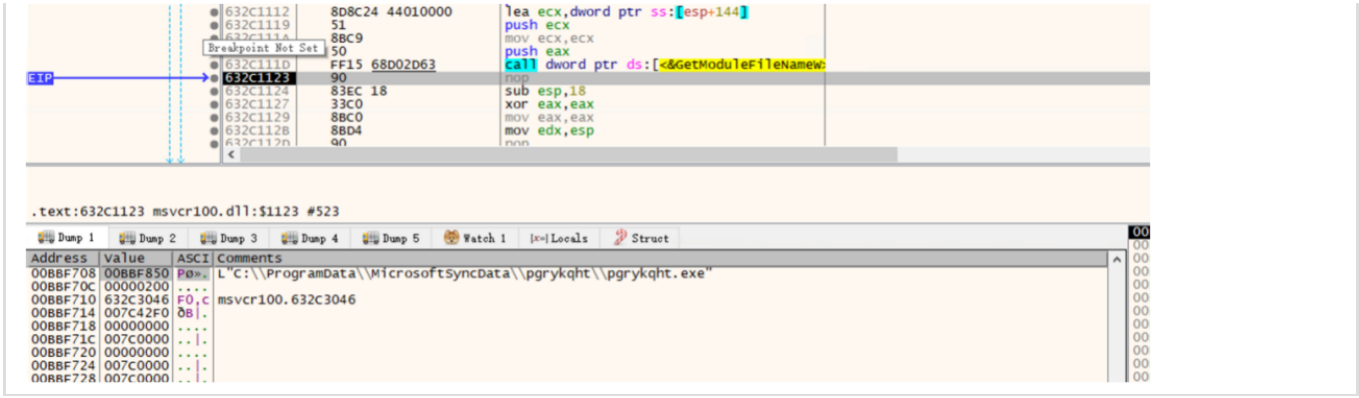
5、创建计划任务

初始化COM，通过COM创建计划任务，参数1:CLSID:**{0f87369f-a4e5-4cfc-bd3e-73e6154572dd}**。

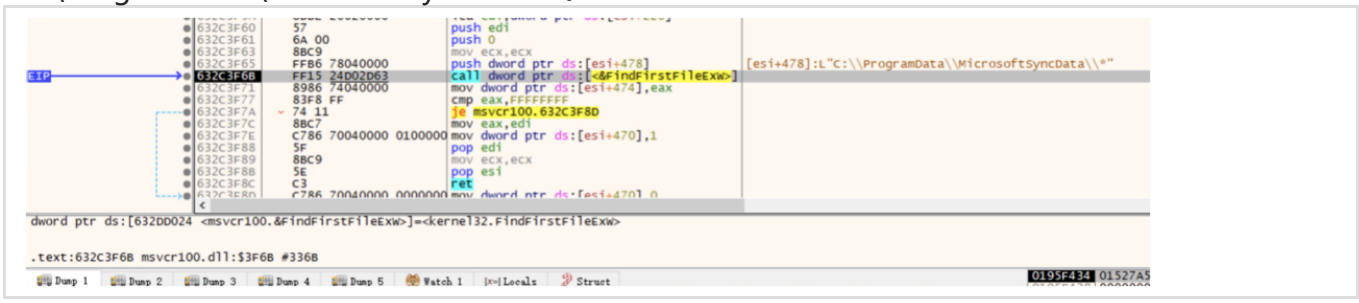


6、释放资源 pgrykqht 分析

获取主进程绝对路径。

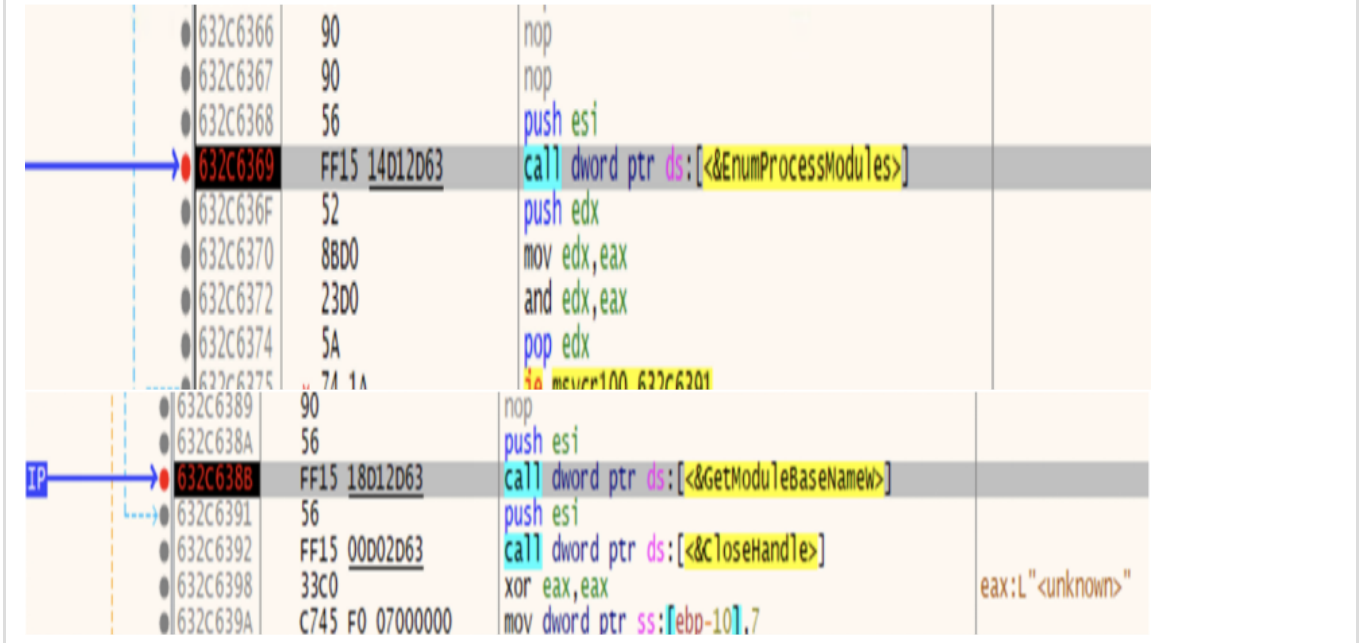


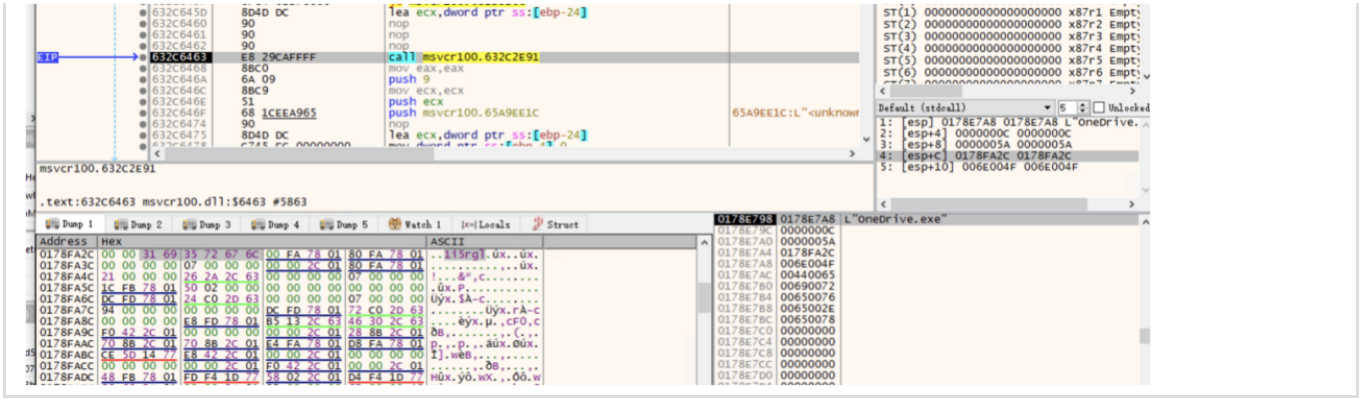
遍历目录
“C:\ProgramData\MicrosoftSyncData*”。



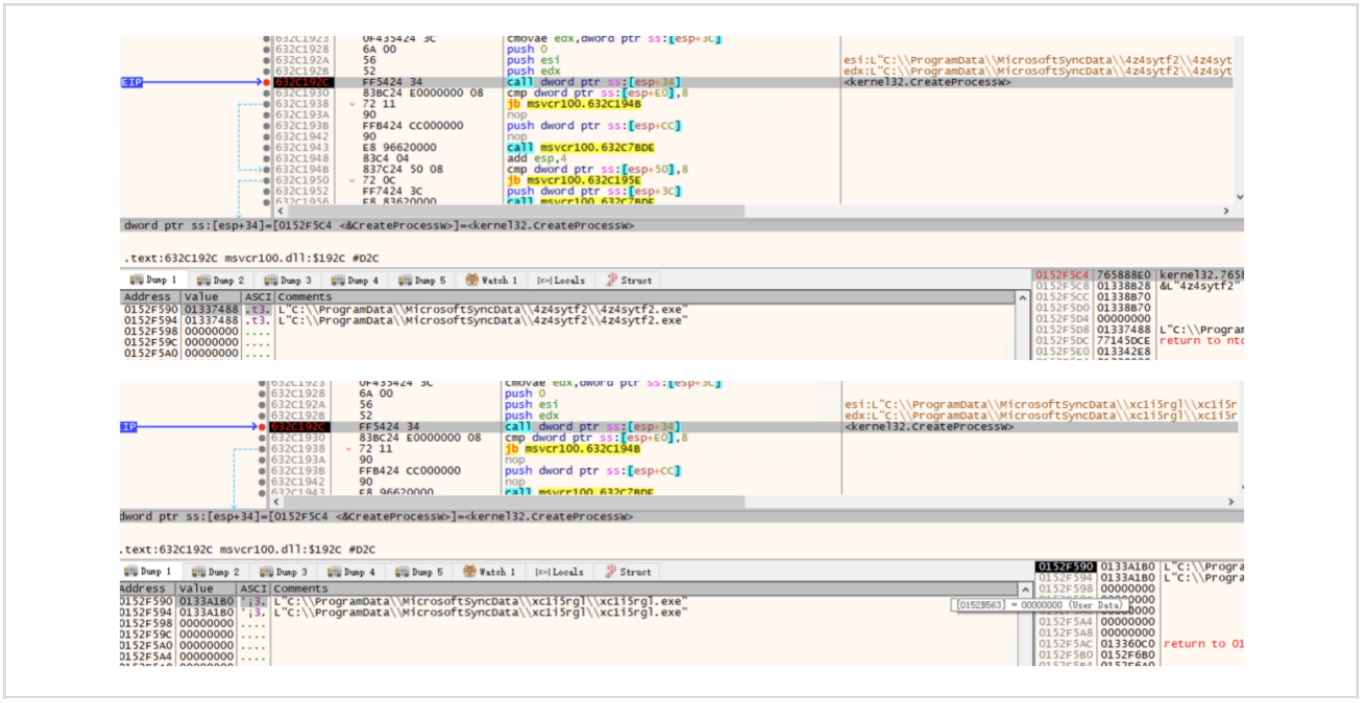
枚举进程列表。

尝试遍历所有进程，通过匹配进程名是否包含资源字符串，判断需守护的进程是否启动。

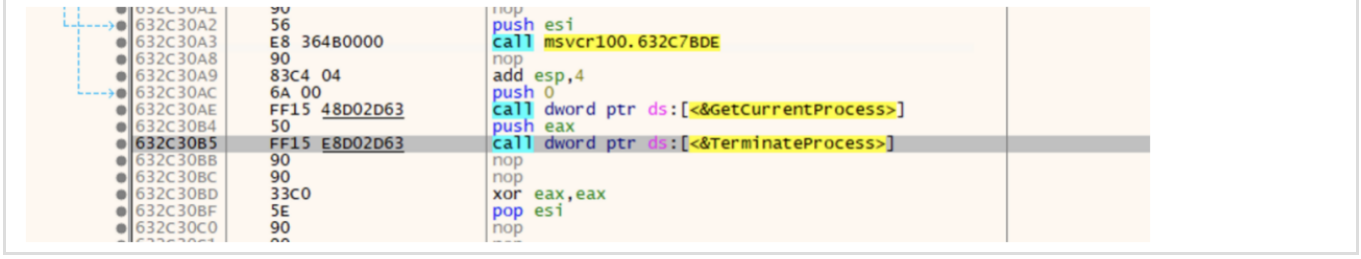




如果两个指定进程未启动就起起来。

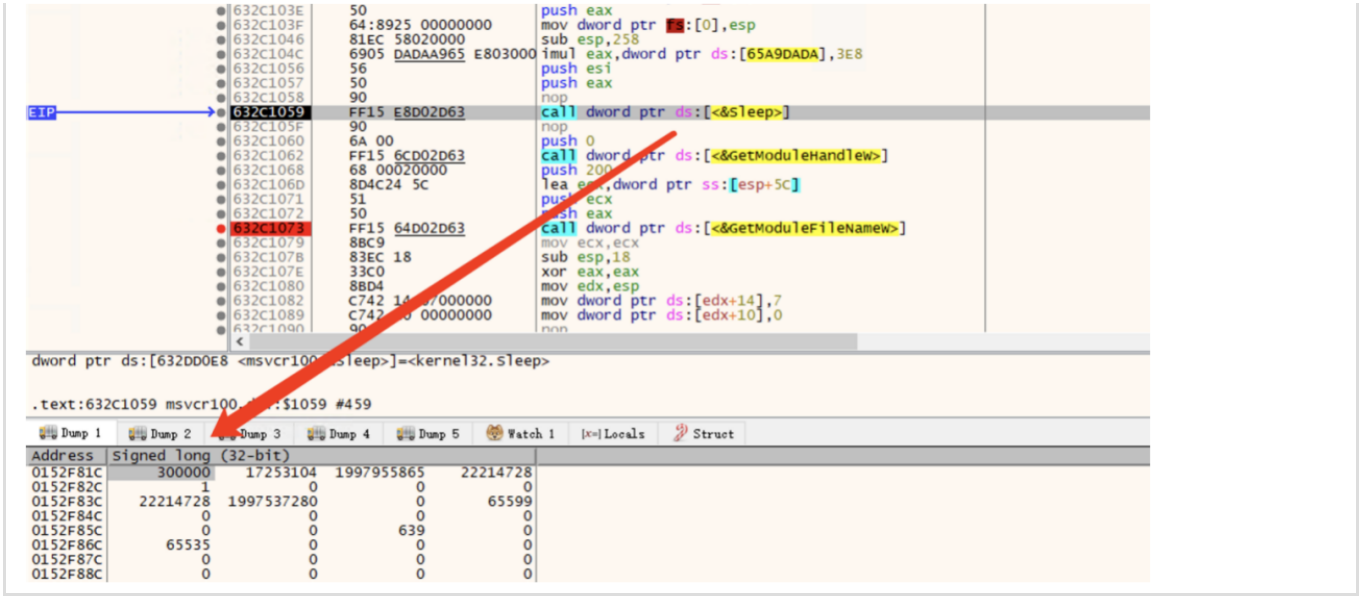


结束自身进程。

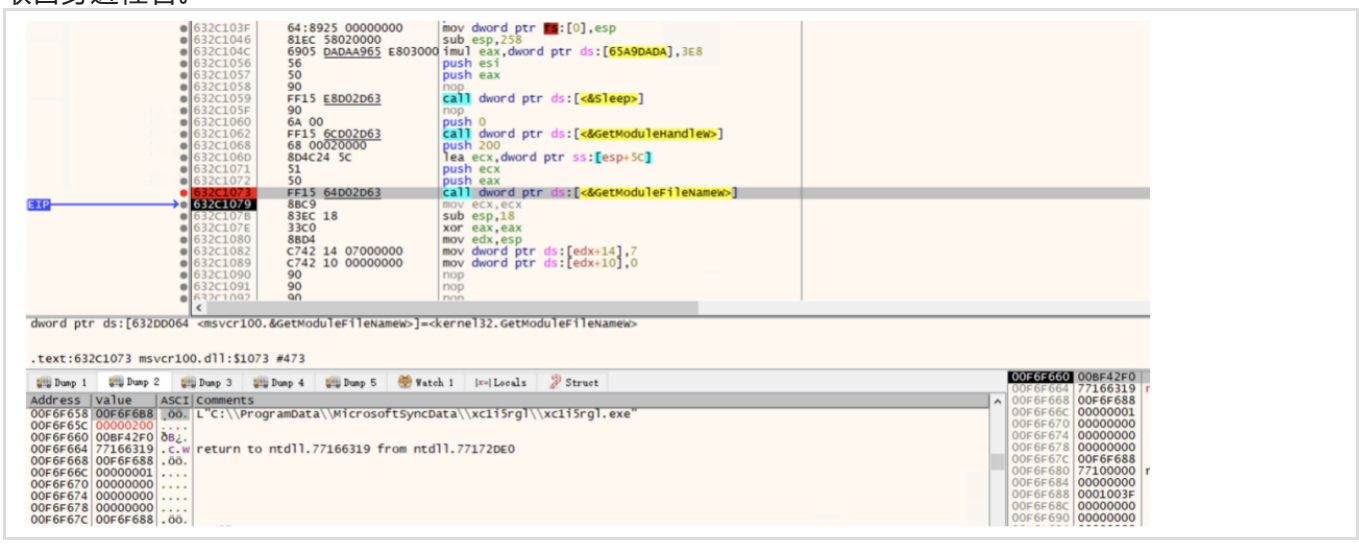


7、释放资源 xc1i5rgl 分析

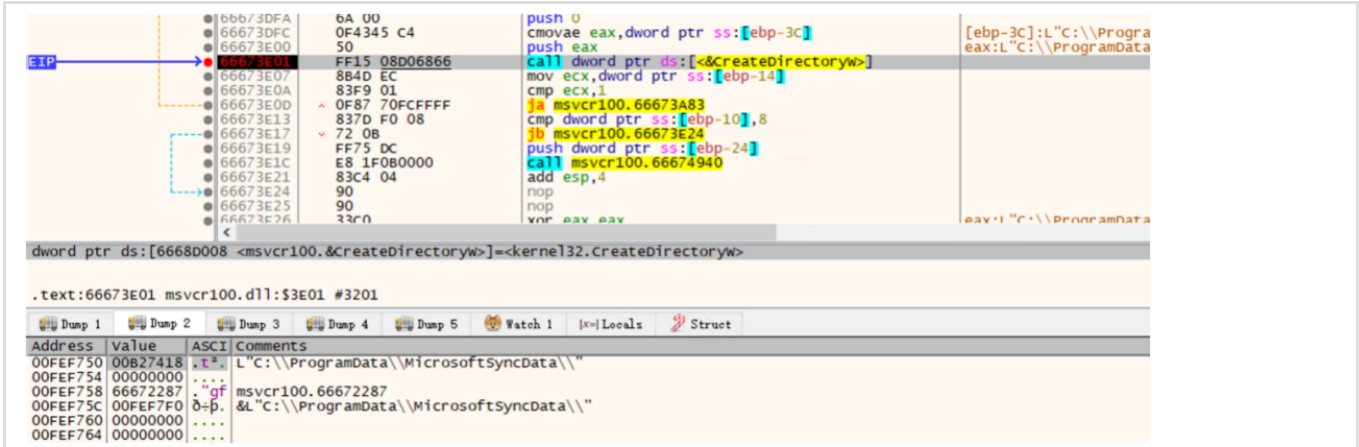
启动后Sleep 300秒。



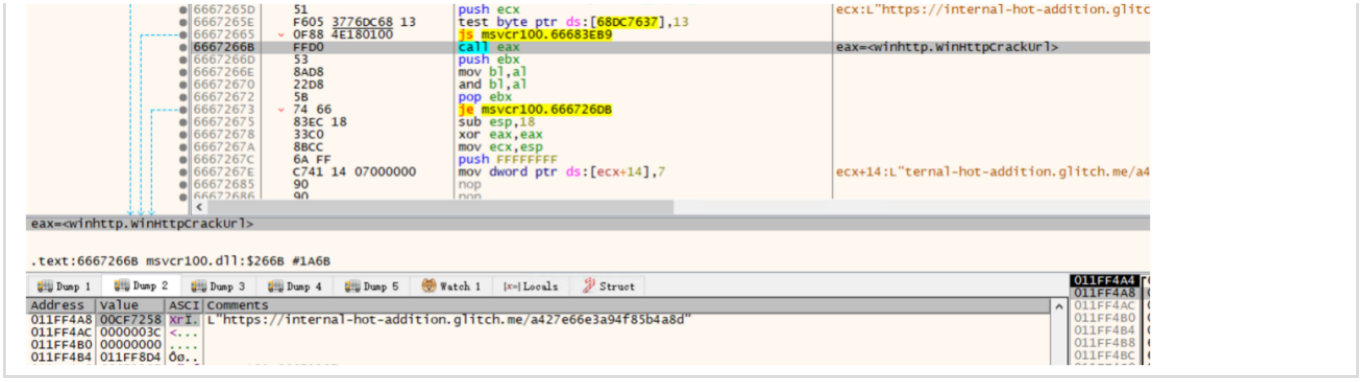
取自身进程名。



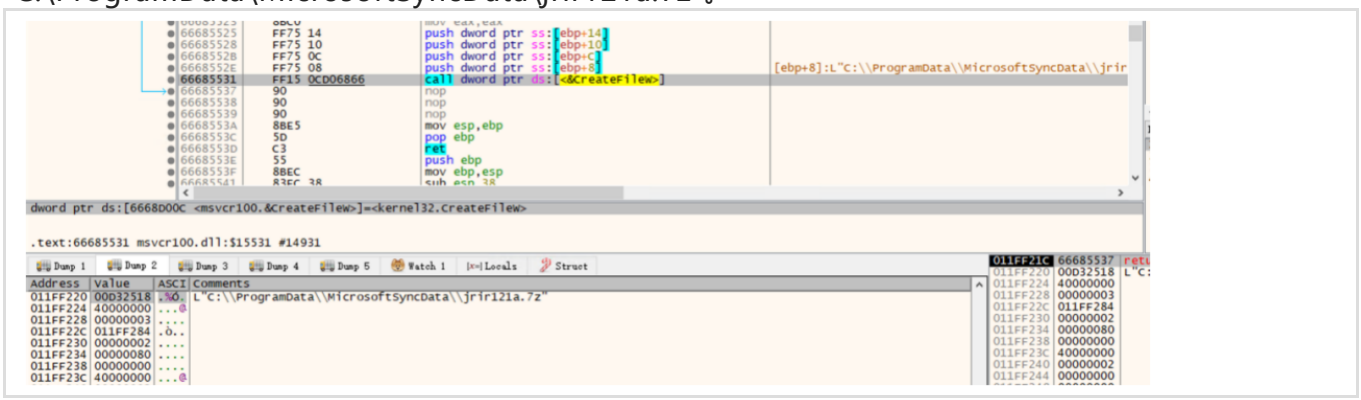
尝试创建路径。



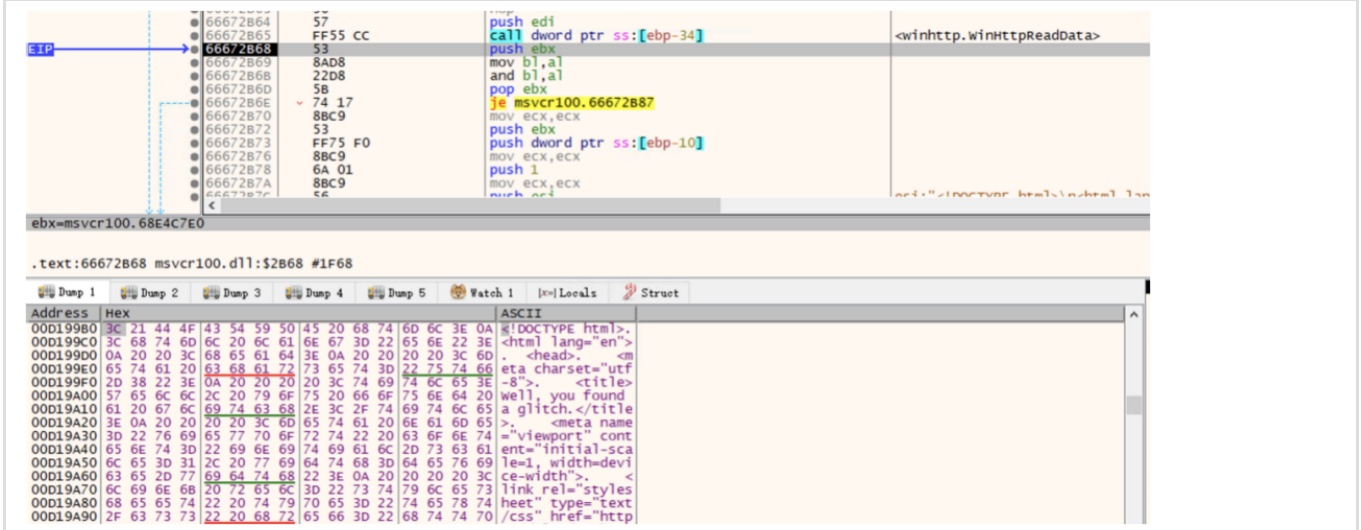
尝试解析URL
“https://internal-hot-addition.glitch.me/a427e66e3a94f85b4a8d”。



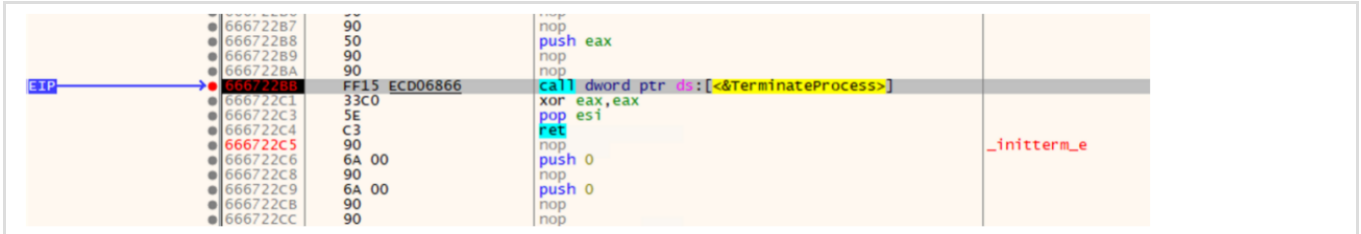
发起HTTP Get请求，下载文件。创建文件“C:\ProgramData\MicrosoftSyncData\jrir121a.7z”。



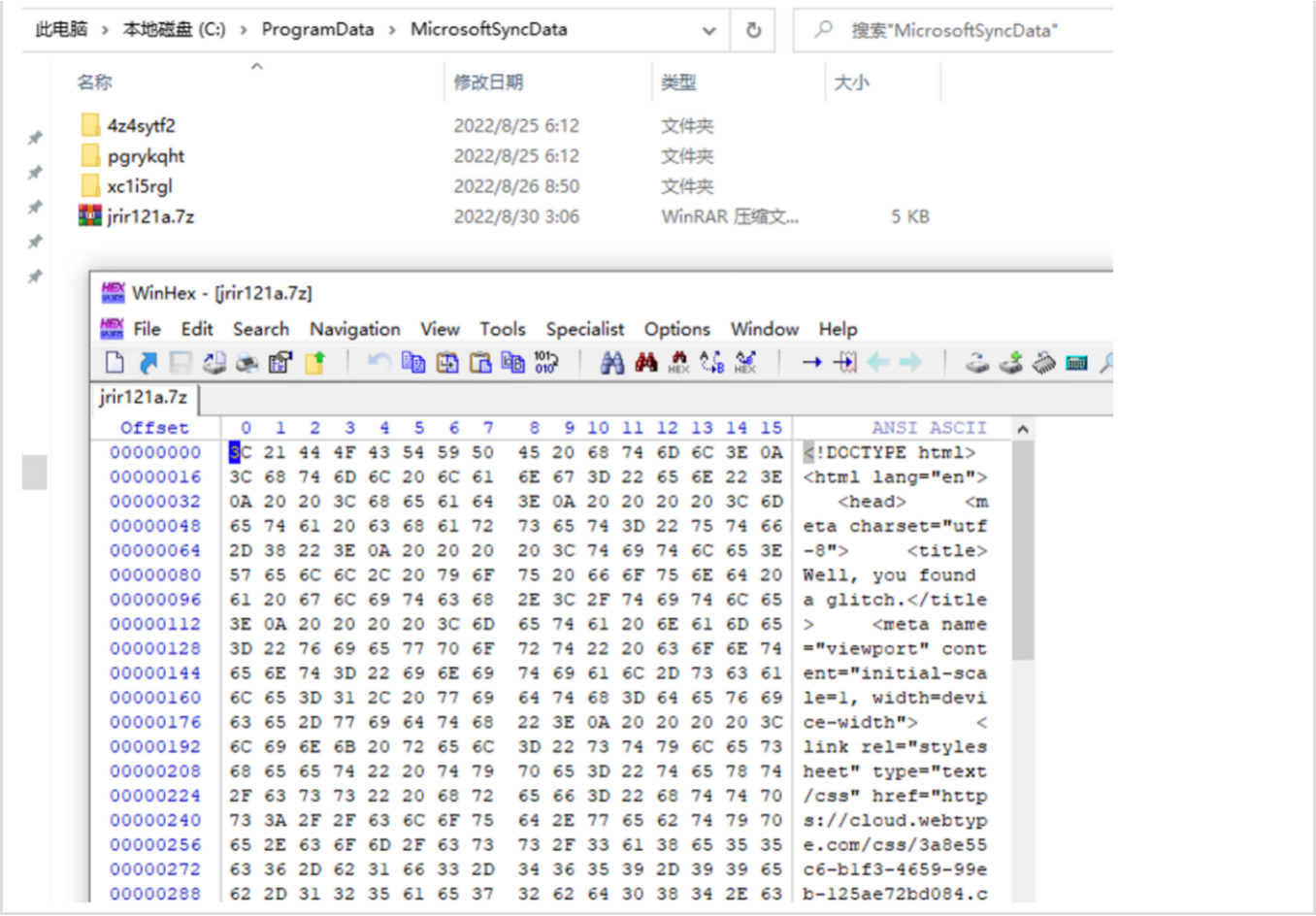
获取返回数据保存到文件，由于文件已被删除，只获取到错误页面的html代码。



结束进程。

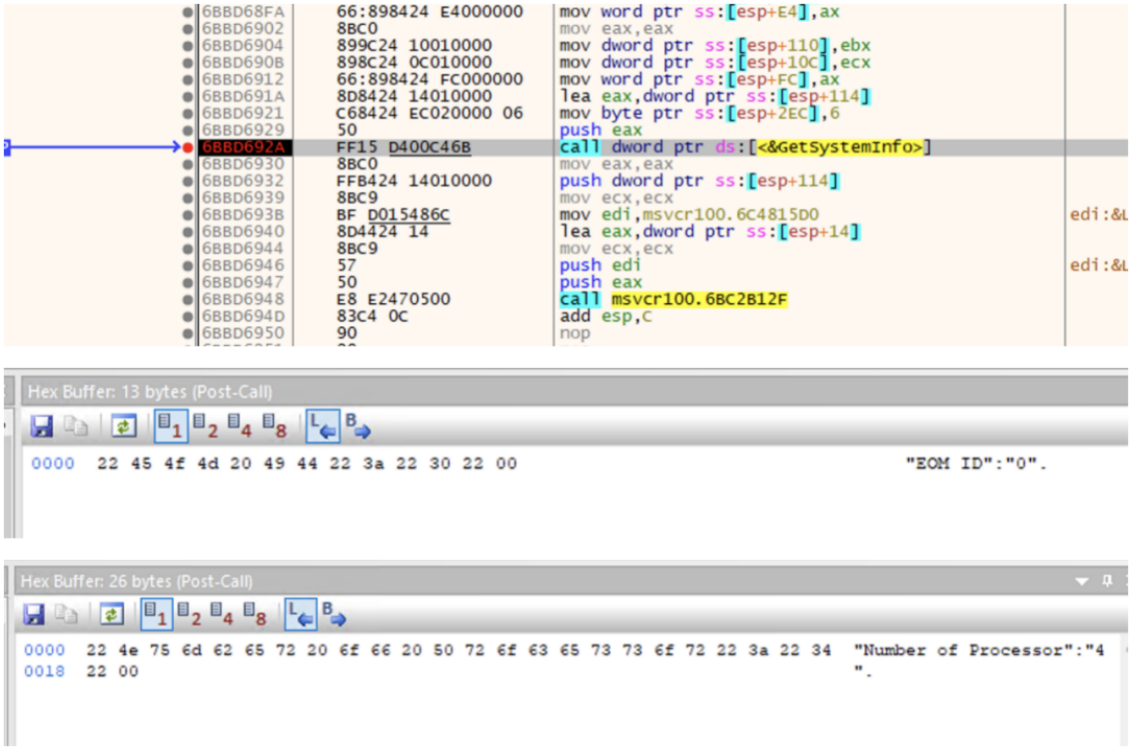


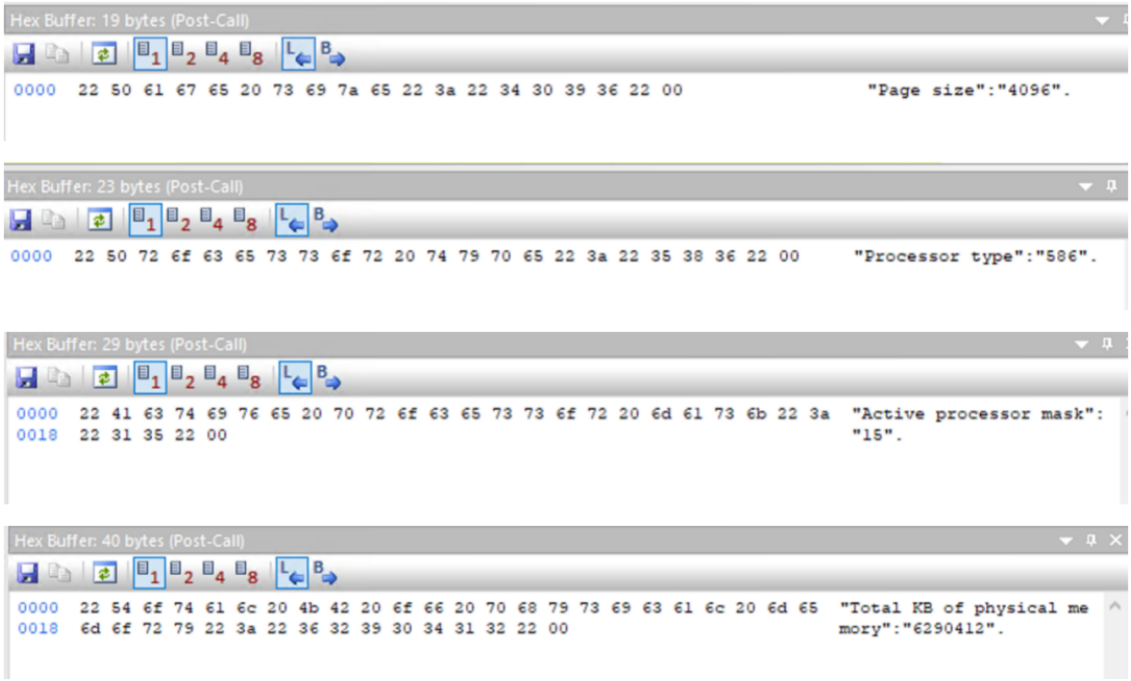
保存下来的文件信息，因为三阶段下载压缩包已失效，导致无法下载正常的压缩包，如下图所示：



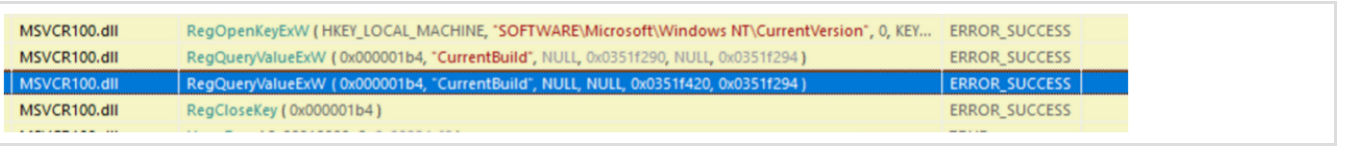
8、释放资源 4z4sytf2 分析

搜集系统信息。



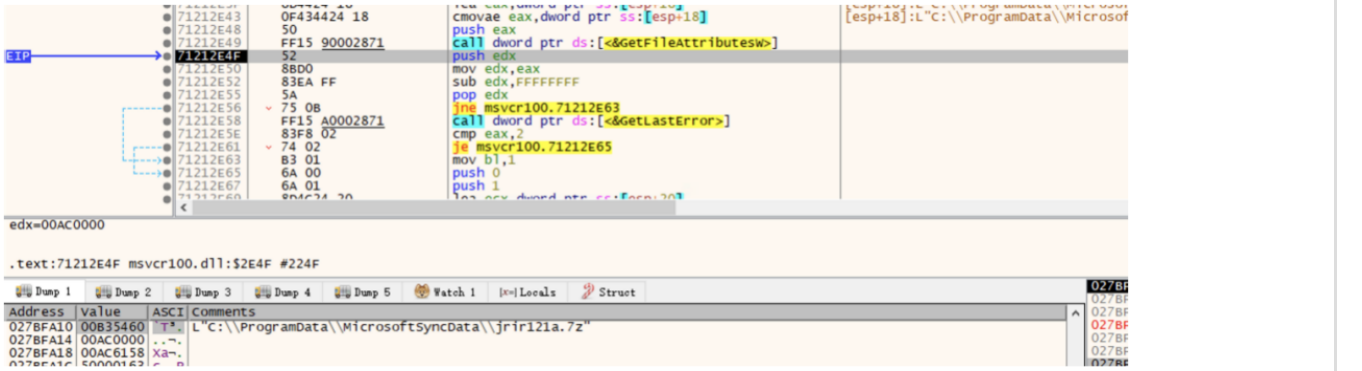


读注册表，获取系统版本号。

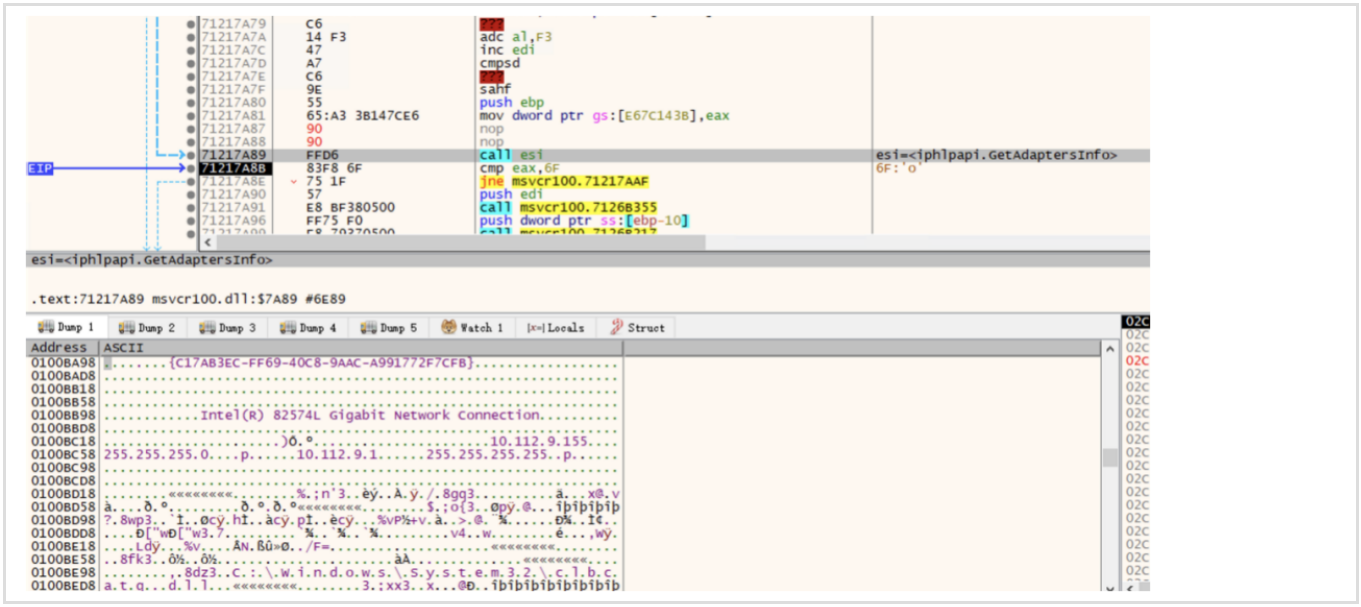


通过com调用wmi 搜集主机信息。

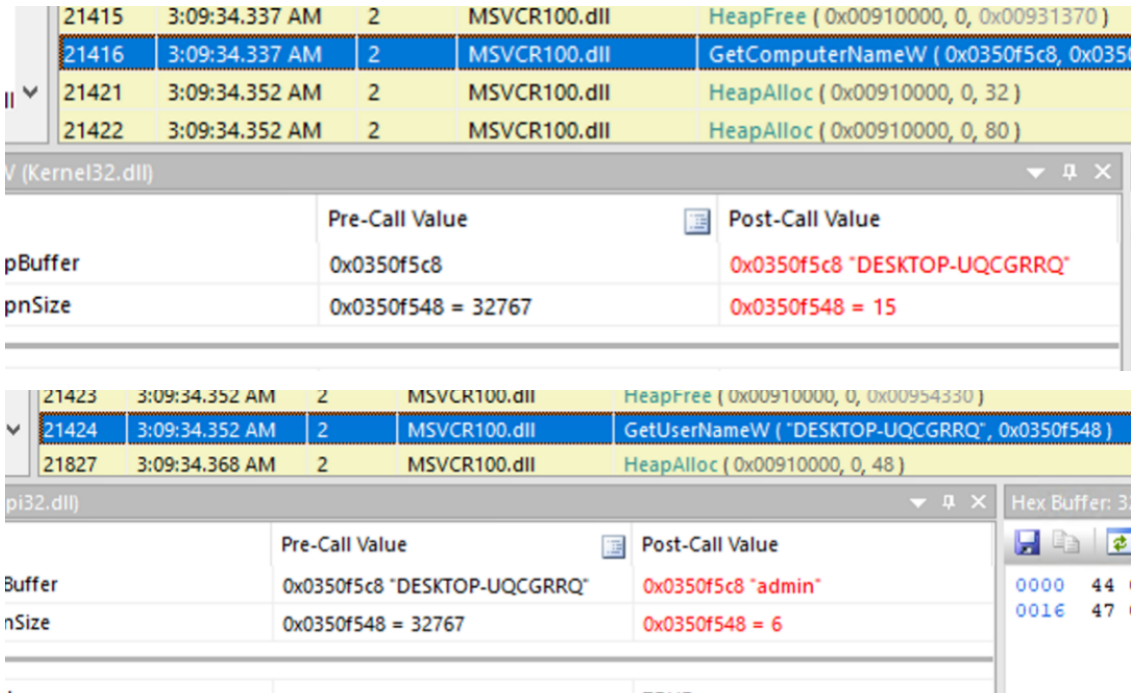
判断文件是否存在
"C:\ProgramData\MicrosoftSyncData\jrir121a.7z"。



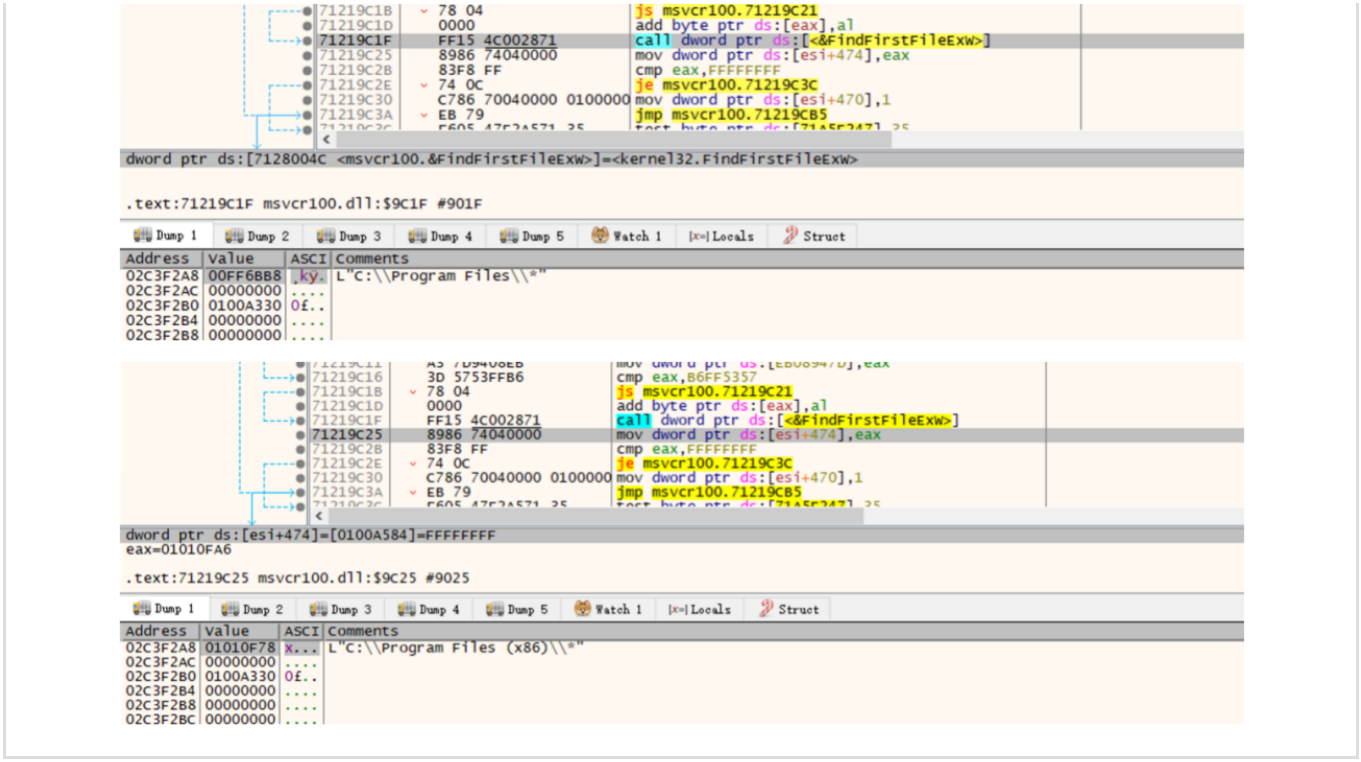
搜集网络相关信息。



搜集主机名与当前用户名。



遍历应用安装目录：
C:\Program Files*
C:\Program Files (x86)*

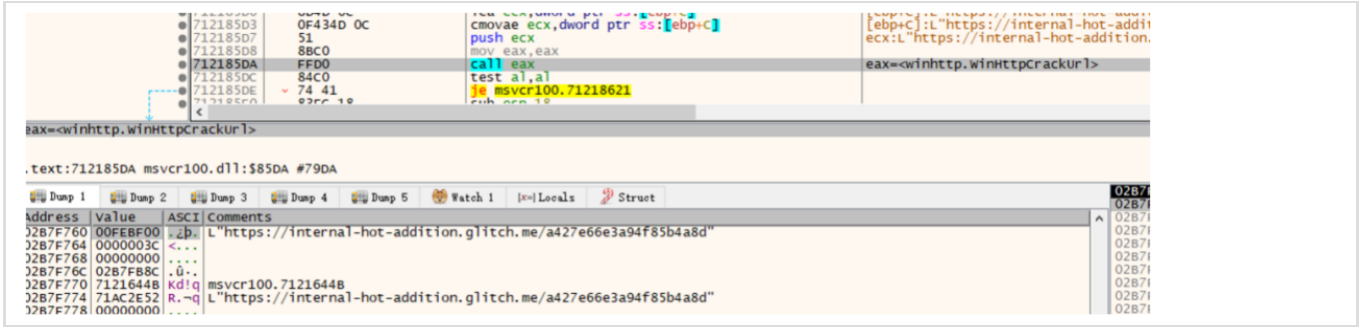


加密采集到的数据。

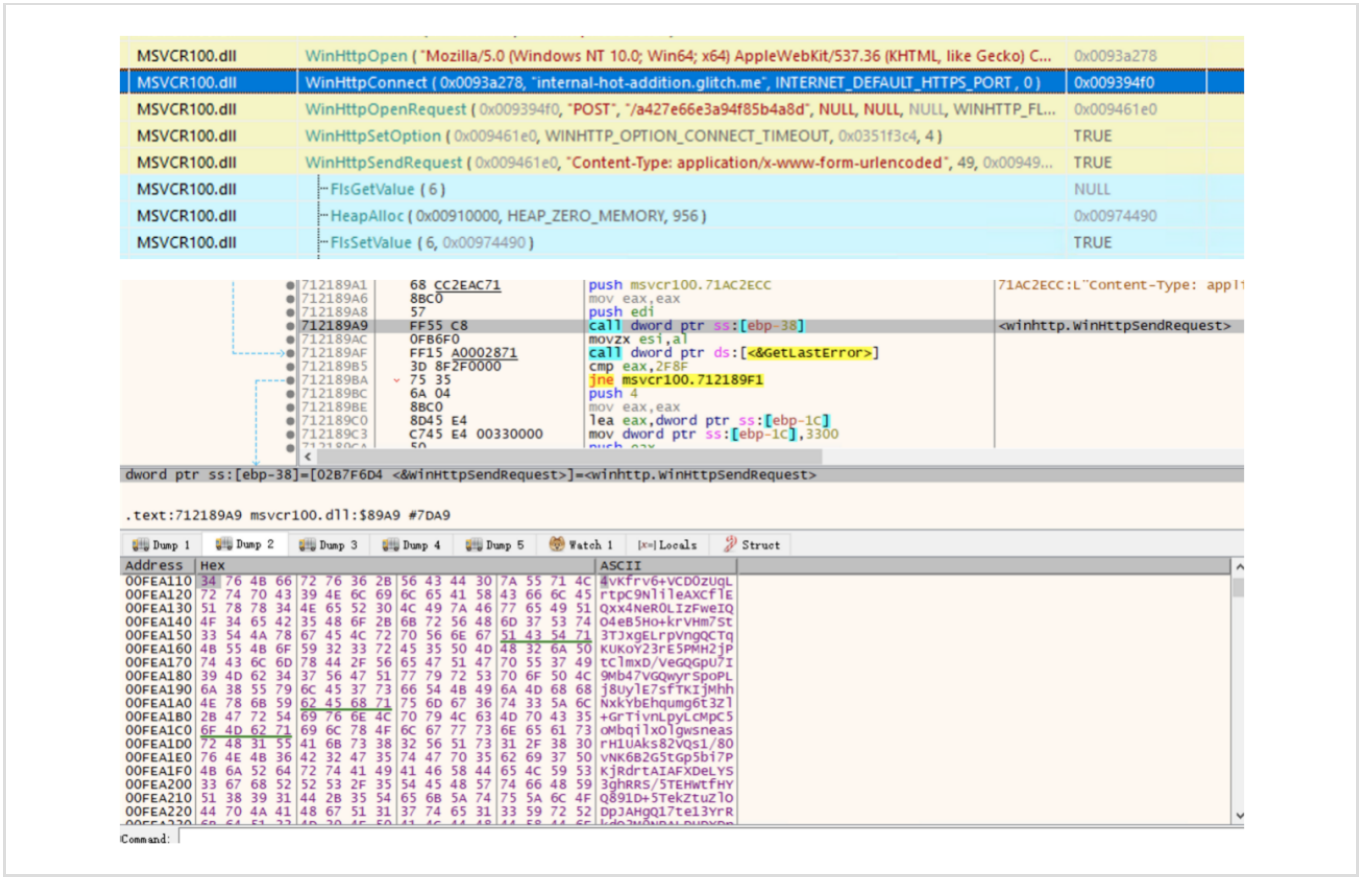
解析URL，准备回传搜集到的数据 。

```
"https://internal-hot-addition.glitch.me/a427e66e3a94f85b4a8d
```

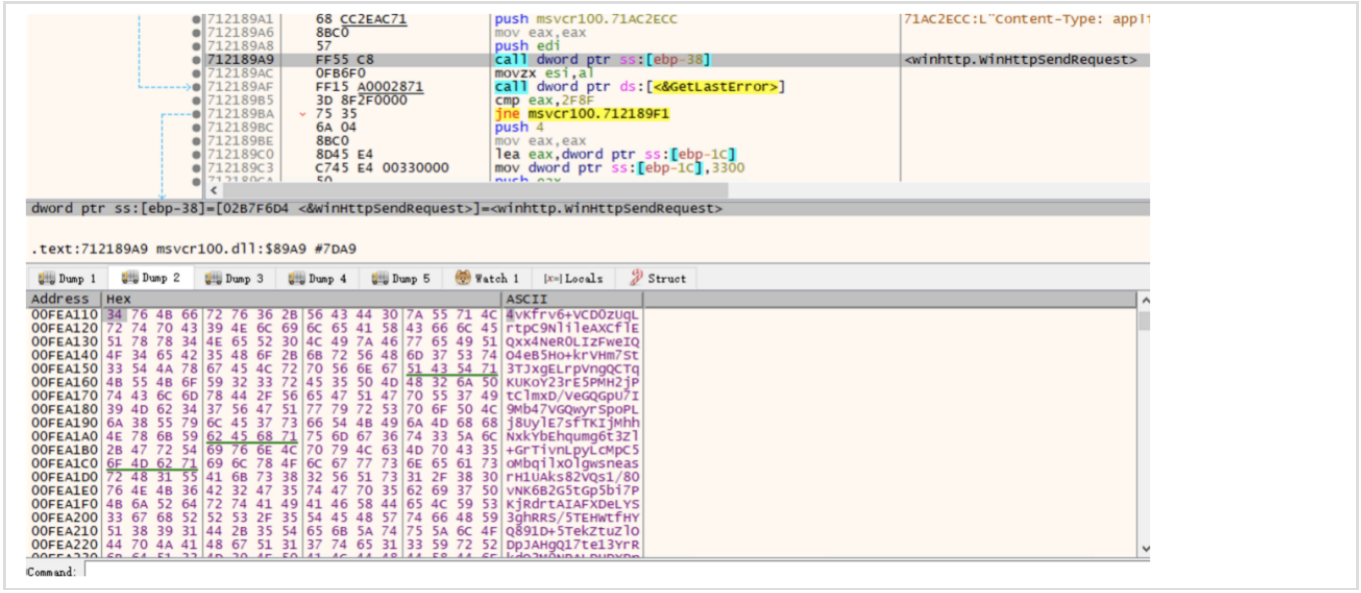
*左右滑动查看更多



通过POST 回传搜集到的数据。



尝试解压下载的7z文件。



由于缺失7z文件内容导致解压失败，中断流程。后续流程为解压执行。

三、关联分析

根据样本行为特征、C2以及结合开源情报，发现此次攻击活动背后的组织为“海莲花”APT。

1、白加黑利用

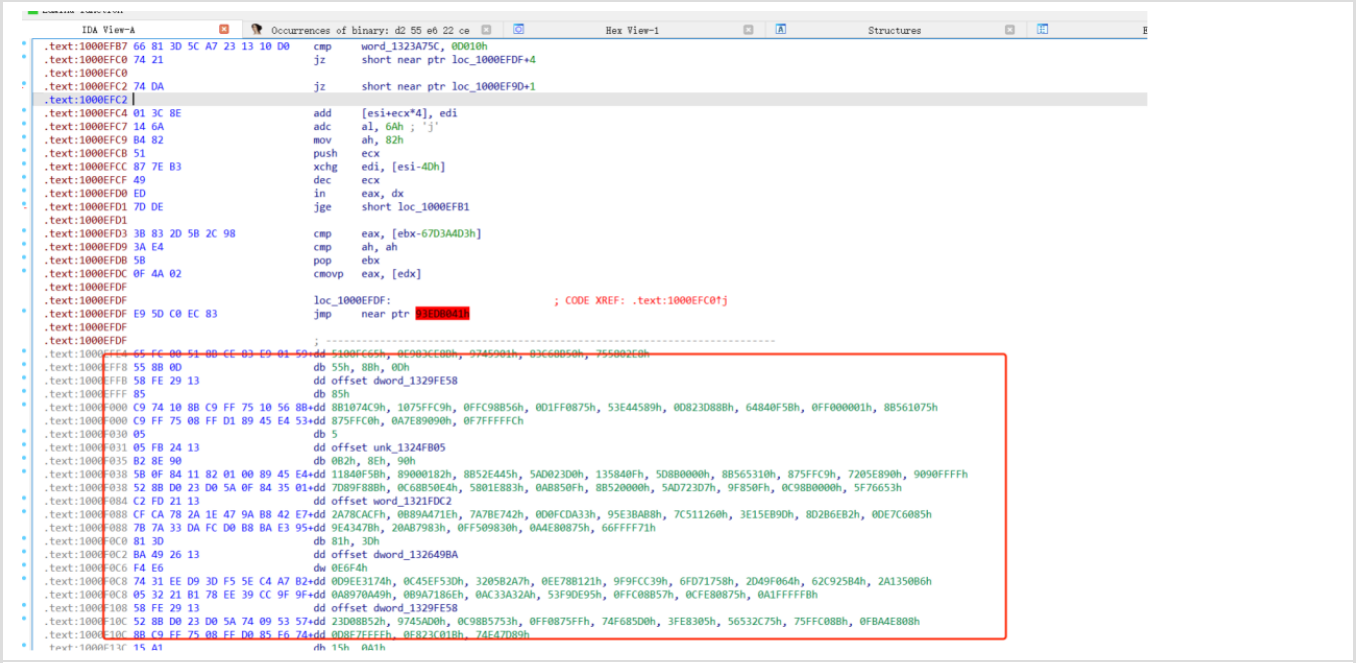
海莲花会使用一系列白加黑利用手法进行防御规避，例如MsMpEng.exe + MpSvc.dll、Sysinternals DebugView tool、the McAfee on-demand scanner、winword+wwlib.dll等。

本次攻击活动样本同样使用了白加黑手法，白文件为Office WINWORD.EXE，黑文件为MSVCR100.dll。

2、代码混淆

海莲花经常使用各种代码混淆手段对抗静态分析。

本次攻击活动样本同样使用了代码混淆手段，样本通过不透明谓词、花指令等方案对抗静态分析。



3、样本行为

2022年1月，Netskope Threat Labs披露的海莲花攻击活动中，恶意文件“background.dll”，创建名为“Winrar Update”的计划任务，每10分钟执行一次。有效负载运行后，首先会收集有关环境的信息，例如网络适配器信息、用户名、计算机名称等。此外，后门还会枚举所有系统的目录和文件，并收集有关运行进程的信息。收集的数据被发送到托管在Glitch上的C2服务器。

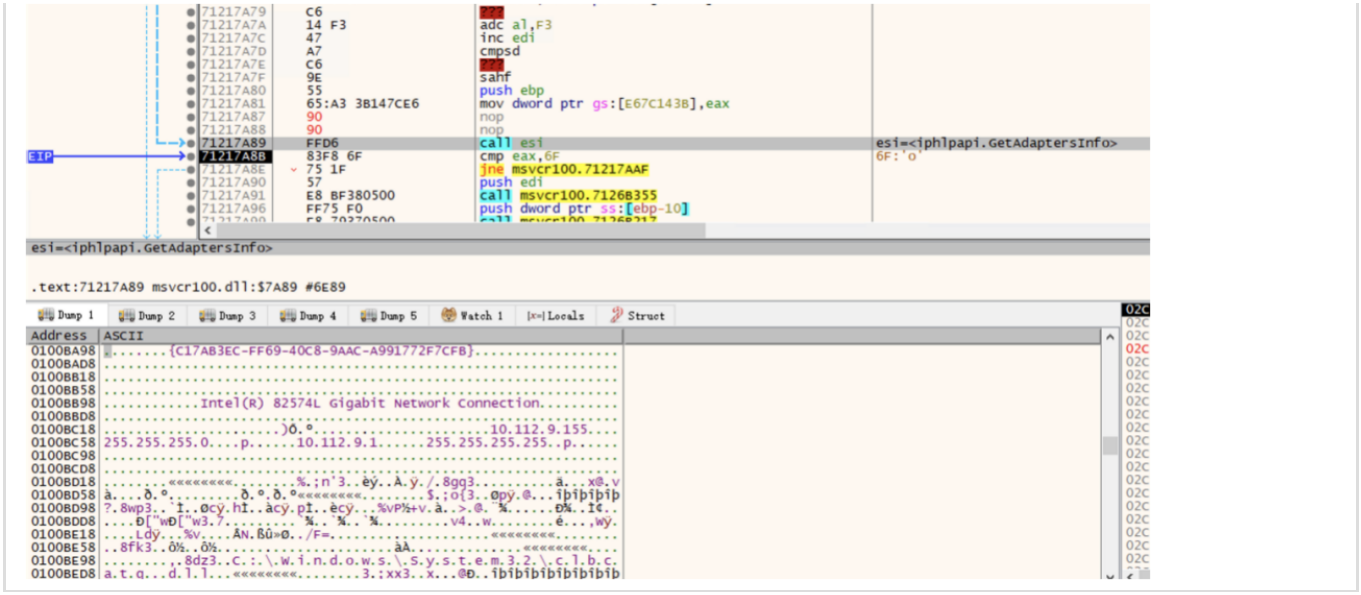
```
阅读网址：

https://www.netskope.com/blog/abusing-microsoft-office-using-malicious-web-archive
```

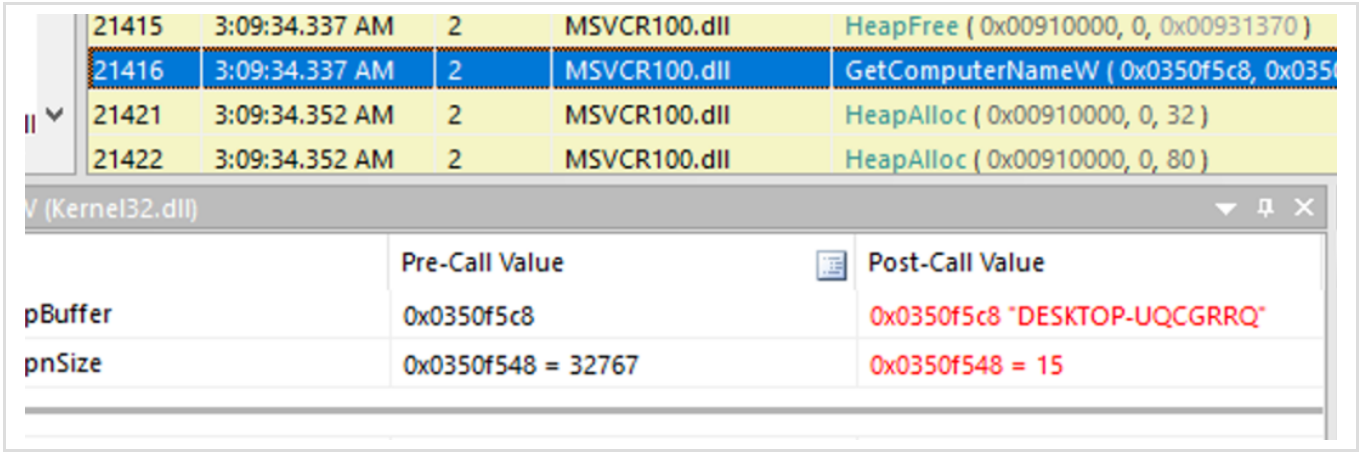
*左右滑动查看更多

本次攻击活动样本同样会收集有关环境的信息。

搜集网络相关信息。



搜集主机名与当前用户名。



4、C2服务器

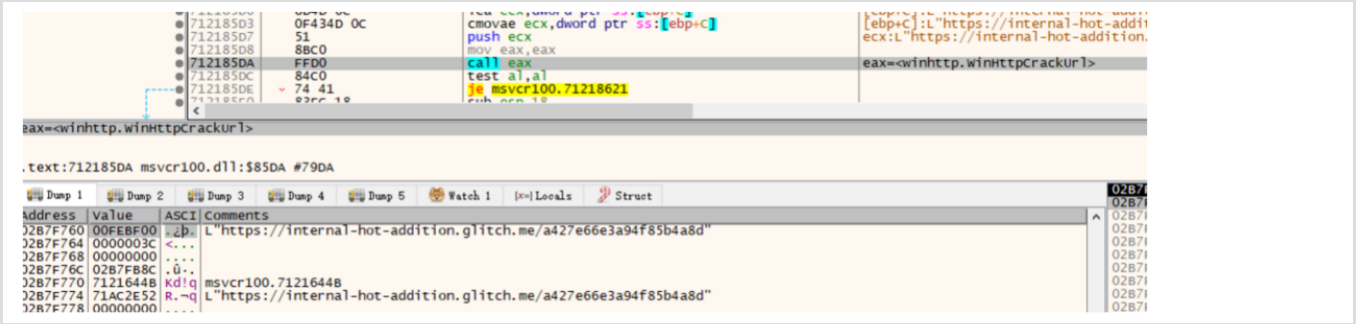
Netskope Threat Labs披露的海莲花攻击活动中的C2服务器：

```
hxxps://confusion-cerulean-samba.glitch[.]me/0627f41878D
hxxps://confusion-cerulean-samba.glitch[.]me/192f188023
hxxps://confusion-cerulean-samba.glitch[.]me/2e06bb0ce9
hxxps://confusion-cerulean-samba.glitch[.]me/55da2c2031
hxxps://confusion-cerulean-samba.glitch[.]me/e1db93941c
hxxps://elemental-future-cheetah.glitch[.]me/559084b660P
hxxps://elemental-future-cheetah.glitch[.]me/afe92a2bd2P
hxxps://torpid-resisted-sugar.glitch[.]me/5db81501e9P
hxxps://torpid-resisted-sugar.glitch[.]me/fb3b5e76b4P
```

*左右滑动查看更多

本次攻击活动样本的C2服务器：

https://internal-hot-addition.glitch.me/a427e66e3a94f85b4a8d



IOC:
HASH:
SHA256:3D46E95284F93BBB76B3B7E1BF0E1B2D51E8A9411C2B6E649112F22F92DE63C2（WINWORD.exe）
SHA256:46eecbbb37a99c735403c17141b21423e39032c53812b8a70446f43aa3ed0a0a（MSVCR100.dll）

C2:
https://internal-hot-addition.glitch[.]me/a427e66e3a94f85b4a8d

四、参考资料及推荐阅读

1.Abusing Microsoft Office Using Malicious Web Archive Files

```
https://www.netskope.com/blog/abusing-microsoft-office-using-malicious-web-archive
```

*左右滑动查看更多

2.Taking Action Against Hackers in Bangladesh and Vietnam

```
https://about.fb.com/news/2020/12/taking-action-against-hackers-in-bangladesh-and-
```

*左右滑动查看更多

3.2021年上半年全球高级持续性威胁（APT）研究报告》

```
http://www.anquan419.com/news/21/839.html
```

*左右滑动查看更多