



山

山

山

山

山

山

山

山

山

W

W

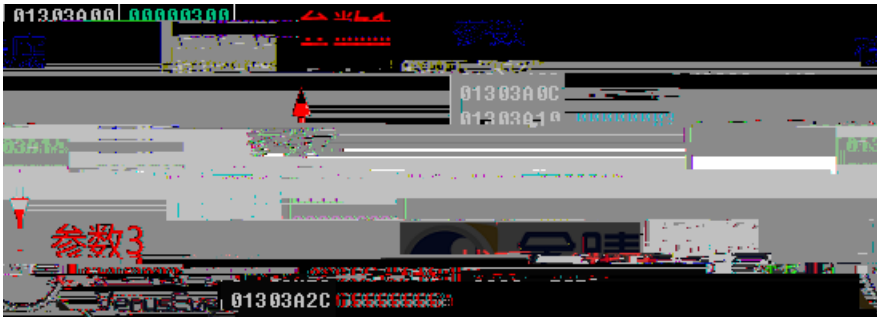
W

W

W

W

地址	数值	注释
00181618	01303A00	
00181619	00000000	← 参数个数
00181620	00000000	
00181621	00000000	



Э

Ю

Ш

Ш

Ш

026A5F40	026A5F44	
026A5F44	6B5AB522	EPSIMP32.6B5AB522
026A5F48	6B5E9E30	EPSIMP32.6B5E9E30
026A5F4C	00000000	
026A5F50	00000000	
026A5F54	6B5E9E2F	EPSIMP32.6B5E9E2F
026A5F58	76ED5F18	ntdll.ZwProtectVirtualMemory
026A5F5C	026A6140	
026A5F60	FFFFFFFF	
026A5F64	026A6040	

三

6B5D1218	E8 46B0FDFF	call EPSIMP32.6B5AC263
6B5D121D	C745 D8 170000	mov dword ptr ss:[ebp-0x28],0x17
6B5D1220	call EPSIMP32.6B5D11EF	
6B5D1224	mov dword ptr ss:[ebp-0x28]	
6B5D1228	mov dword ptr [eax-0x12]	
6B5D122C	call Winsock2.224E484C (Winsock2.224E484C)	
6B5D122E	3BC7	cmp eax,edi
6B5D1230	75 49	jg EPSIMP32.6B5D1235
6B5D1234	0F 22K	or eax,0xFFFFFFFF
026A5F40	026A5F44	
026A5F44	6B5AB522	EPSIMP32.6B5AB522
026A5F48	6B5E9E30	EPSIMP32.6B5E9E30

WWWW

00412E41	6A 01	push 0x1	
00412E43	33D2	xor edx,edx	
00412E45	B9 E8974200	mov ecx,0x4297E8	WINWORD.exe
00412E4A	E8 82FEFFFF	call 00412CD1	
00412E4F	59	pop ecx	0041348C
00412E50	8BC8	mov ecx,eax	
00412E52	E8 14FDFFFF	call 00412B6B	
00412E57	85C0	test eax,eax	
00412E59	00412F27		
00412E61	E8 5CFDFFFF		004128C2

山

```

00412E04 57          push edi
s:[ebp-0x10]
short 00412F04
eax 0x00000000
push ecx
push ecx
push ecx
call dword ptr s

```

山

```

54 do
55 {
// 将dll文件保存到临时目录
// 判断是否通过rundll32执行dll

```

山

山

```

15 v0[1] = 50;
16 lpString2 = (LPCWSTR)decrypt((int)v0); // "apisecconnect.dll"
17 *v0 = aB0A;
18 v0[1] = 10;
20 lpString2 = (LPCWSTR)decrypt((int)v0); // "apisecconnect.dll"
21 lpString2 = (LPCWSTR)decrypt((int)v0);
22 CONST WCHAR * lpString2 = (LPCWSTR)decrypt((int)v0);
23 lpString2 = (LPCWSTR)decrypt((int)v0);
24 lpString2 = (LPCWSTR)decrypt((int)v0);
25 lpString2 = (LPCWSTR)decrypt((int)v0);
26 lpString2 = (LPCWSTR)decrypt((int)v0);
27 lpString2 = (LPCWSTR)decrypt((int)v0);
28 lpString2 = (LPCWSTR)decrypt((int)v0);
29 lpString2 = (LPCWSTR)decrypt((int)v0);
30 lpString2 = (LPCWSTR)decrypt((int)v0);
31 lpString2 = (LPCWSTR)decrypt((int)v0);
32 lpString2 = (LPCWSTR)decrypt((int)v0);
33 lpString2 = (LPCWSTR)decrypt((int)v0);
34 lpString2 = (LPCWSTR)decrypt((int)v0);
35 lpString2 = (LPCWSTR)decrypt((int)v0);
36 lpString2 = (LPCWSTR)decrypt((int)v0);
37 lpString2 = (LPCWSTR)decrypt((int)v0);
38 lpString2 = (LPCWSTR)decrypt((int)v0);
39 lpString2 = (LPCWSTR)decrypt((int)v0);
40 lpString2 = (LPCWSTR)decrypt((int)v0);
41 lpString2 = (LPCWSTR)decrypt((int)v0);
42 lpString2 = (LPCWSTR)decrypt((int)v0);
43 lpString2 = (LPCWSTR)decrypt((int)v0);
44 lpString2 = (LPCWSTR)decrypt((int)v0);
45 lpString2 = (LPCWSTR)decrypt((int)v0);
46 lpString2 = (LPCWSTR)decrypt((int)v0);
47 lpString2 = (LPCWSTR)decrypt((int)v0);
48 lpString2 = (LPCWSTR)decrypt((int)v0);
49 lpString2 = (LPCWSTR)decrypt((int)v0);
50 lpString2 = (LPCWSTR)decrypt((int)v0);
51 lpString2 = (LPCWSTR)decrypt((int)v0);
52 lpString2 = (LPCWSTR)decrypt((int)v0);
53 lpString2 = (LPCWSTR)decrypt((int)v0);
54 lpString2 = (LPCWSTR)decrypt((int)v0);
55 lpString2 = (LPCWSTR)decrypt((int)v0);
56 lpString2 = (LPCWSTR)decrypt((int)v0);
57 lpString2 = (LPCWSTR)decrypt((int)v0);
58 lpString2 = (LPCWSTR)decrypt((int)v0);
59 lpString2 = (LPCWSTR)decrypt((int)v0);
60 lpString2 = (LPCWSTR)decrypt((int)v0);
61 lpString2 = (LPCWSTR)decrypt((int)v0);
62 lpString2 = (LPCWSTR)decrypt((int)v0);
63 lpString2 = (LPCWSTR)decrypt((int)v0);
64 lpString2 = (LPCWSTR)decrypt((int)v0);
65 lpString2 = (LPCWSTR)decrypt((int)v0);
66 lpString2 = (LPCWSTR)decrypt((int)v0);
67 lpString2 = (LPCWSTR)decrypt((int)v0);
68 lpString2 = (LPCWSTR)decrypt((int)v0);
69 lpString2 = (LPCWSTR)decrypt((int)v0);
70 lpString2 = (LPCWSTR)decrypt((int)v0);
71 lpString2 = (LPCWSTR)decrypt((int)v0);
72 lpString2 = (LPCWSTR)decrypt((int)v0);
73 lpString2 = (LPCWSTR)decrypt((int)v0);
74 lpString2 = (LPCWSTR)decrypt((int)v0);
75 lpString2 = (LPCWSTR)decrypt((int)v0);
76 lpString2 = (LPCWSTR)decrypt((int)v0);
77 lpString2 = (LPCWSTR)decrypt((int)v0);
78 lpString2 = (LPCWSTR)decrypt((int)v0);
79 lpString2 = (LPCWSTR)decrypt((int)v0);
80 lpString2 = (LPCWSTR)decrypt((int)v0);
81 lpString2 = (LPCWSTR)decrypt((int)v0);
82 lpString2 = (LPCWSTR)decrypt((int)v0);
83 lpString2 = (LPCWSTR)decrypt((int)v0);
84 lpString2 = (LPCWSTR)decrypt((int)v0);
85 lpString2 = (LPCWSTR)decrypt((int)v0);
86 lpString2 = (LPCWSTR)decrypt((int)v0);
87 lpString2 = (LPCWSTR)decrypt((int)v0);
88 lpString2 = (LPCWSTR)decrypt((int)v0);
89 lpString2 = (LPCWSTR)decrypt((int)v0);
90 lpString2 = (LPCWSTR)decrypt((int)v0);
91 lpString2 = (LPCWSTR)decrypt((int)v0);
92 lpString2 = (LPCWSTR)decrypt((int)v0);
93 lpString2 = (LPCWSTR)decrypt((int)v0);
94 lpString2 = (LPCWSTR)decrypt((int)v0);
95 lpString2 = (LPCWSTR)decrypt((int)v0);
96 lpString2 = (LPCWSTR)decrypt((int)v0);
97 lpString2 = (LPCWSTR)decrypt((int)v0);
98 lpString2 = (LPCWSTR)decrypt((int)v0);
99 lpString2 = (LPCWSTR)decrypt((int)v0);
100 lpString2 = (LPCWSTR)decrypt((int)v0);

```

