



00011C80	\$ 55	push	ebp	
00011C81	. 89E5	mov	ebp, esp	
00011C83	. 83EC 04	sub	esp, 4	
00011C86	. 64:A1 300000	mov	eax, dword ptr fs:[30]	
00011C8C	. 8B40 68	mov	eax, dword ptr [eax+68]	
00011C8F	. 8945 FC	mov	dword ptr [ebp-4], eax	
00011C92	. 8B45 FC	mov	eax, dword ptr [ebp-4]	
00011C95	. 89EC	mov	esp, ebp	
00011C97	. 5D	pop	ebp	
00011C98	. C3	ret		

00011BAF	00	db	00
00011BB0	\$ 55	push	ebp
00011BB1	. 89E5	mov	ebp, esp
00011BB3	. CD 01	int	1
00011BB5	. B8 55730880	mov	eax, 80087355
00011BBA	. FFE0	jmp	eax
00011BBC	. 89EC	mov	esp, ebp
00011BBE	. 5D	pop	ebp
00011BBF	. C3	ret	
00011BC0	. 55	push	ebp

00011300 . 0745 60 mov dword ptr [ebp+00], eax
00011308 . 8D45 9C lea eax, dword ptr [ebp-64]
0001130B . 50 push eax
0001130C . FF15 9CAB0101 call dword ptr [&USER32.RegisterClassExA] RegisterClassExA
0001130E . 66:85C0 test ax, ax
00011310 . 74 75 jz short 0001143C
00011312 . 6A 00 push 0
00011314 . 56 push esi
00011316 . 6A 00 push 0
00011318 . 6A 00 push 0
0001131A . 6A 78 push 78
0001131C . 68 F0000000 push 0F0
0001131E . DC037E2004 push 00000004
00011320 . 68 0000CF00 push 00000000
00011322 . 50 push eax
00011324 . 68 00000000 push 00000000
00011326 . 50 push eax
00011328 . 68 00000000 push 00000000
0001132A . 50 push eax
0001132C . 68 00000000 push 00000000
0001132E . 50 push eax
00011330 . 68 00000000 push 00000000
00011332 . 50 push eax
00011334 . 68 00000000 push 00000000
00011336 . 50 push eax
00011338 . 68 00000000 push 00000000
0001133A . 50 push eax
0001133C . 68 00000000 push 00000000
0001133E . 50 push eax
00011340 . 68 00000000 push 00000000
00011342 . 50 push eax
00011344 . 68 00000000 push 00000000
00011346 . 50 push eax
00011348 . 68 00000000 push 00000000
0001134A . 50 push eax
0001134C . 68 00000000 push 00000000
0001134E . 50 push eax
00011350 . 68 00000000 push 00000000
00011352 . 50 push eax
00011354 . 68 00000000 push 00000000
00011356 . 50 push eax
00011358 . 68 00000000 push 00000000
0001135A . 50 push eax
0001135C . 68 00000000 push 00000000
0001135E . 50 push eax
00011360 . 68 00000000 push 00000000
00011362 . 50 push eax
00011364 . 68 00000000 push 00000000
00011366 . 50 push eax
00011368 . 68 00000000 push 00000000
0001136A . 50 push eax
0001136C . 68 00000000 push 00000000
0001136E . 50 push eax
00011370 . 68 00000000 push 00000000
00011372 . 50 push eax
00011374 . 68 00000000 push 00000000
00011376 . 50 push eax
00011378 . 68 00000000 push 00000000
0001137A . 50 push eax
0001137C . 68 00000000 push 00000000
0001137E . 50 push eax
00011380 . 68 00000000 push 00000000
00011382 . 50 push eax
00011384 . 68 00000000 push 00000000
00011386 . 50 push eax
00011388 . 68 00000000 push 00000000
0001138A . 50 push eax
0001138C . 68 00000000 push 00000000
0001138E . 50 push eax
00011390 . 68 00000000 push 00000000
00011392 . 50 push eax
00011394 . 68 00000000 push 00000000
00011396 . 50 push eax
00011398 . 68 00000000 push 00000000
0001139A . 50 push eax
0001139C . 68 00000000 push 00000000
0001139E . 50 push eax
000113A0 . 68 00000000 push 00000000
000113A2 . 50 push eax
000113A4 . 68 00000000 push 00000000
000113A6 . 50 push eax
000113A8 . 68 00000000 push 00000000
000113AA . 50 push eax
000113AC . 68 00000000 push 00000000
000113AE . 50 push eax
000113B0 . 68 00000000 push 00000000
000113B2 . 50 push eax
000113B4 . 68 00000000 push 00000000
000113B6 . 50 push eax
000113B8 . 68 00000000 push 00000000
000113BA . 50 push eax
000113BC . 68 00000000 push 00000000
000113BE . 50 push eax
000113C0 . 68 00000000 push 00000000
000113C2 . 50 push eax
000113C4 . 68 00000000 push 00000000
000113C6 . 50 push eax
000113C8 . 68 00000000 push 00000000
000113CA . 50 push eax
000113CC . 68 00000000 push 00000000
000113CE . 50 push eax
000113D0 . 68 F0000000 push 0F0

Call Stack:
RegisterClassExA
lpParam = NULL
hInst = NULL
hMenu = NULL
hParent = NULL
Height = 78 (120.)
Width = F0 (240.)

CPU Registers:
EAX: 00000000
ECX: 00000000
EDI: 00000000
ESI: 00000000

00011270 . 53 push ebx
00011271 . 56 push esi
00011272 . 57 push edi
00011273 . 8B5C24 10 mov ebx, dword ptr [esp+10]
00011277 . 8B7424 14 mov esi, dword ptr [esp+14]
0001127B . 8B7C24 18 mov edi, dword ptr [esp+18]
0001127F . 83FE 01 cmp esi, 1
00011282 . 74 18 je short 0001129C
00011284 . 83FE 02 cmp esi, 2
00011287 . 74 33 je short 000112BC
00011289 . 83FE 01 cmp esi, 1
0001128C . 7C 3A jl short 000112C8
0001128E . 83FE 10 cmp esi, 10
00011291 . 75 35 jnz short 000112C8
00011293 . 53 push ebx
00011294 . FF15 88AB0101 call dword ptr [&USER32.DestroyWindow] DestroyWindow
0001129A . EB 28 jmp short 000112C4
0001129C > E8 AF010000 call 00011450
000112A1 . 6A 00 push 0
000112A3 . FF35 00A00101 call dword ptr [1A000]
000112A9 . 50 push eax
000112AA . E8 11020000 call 000114C0
000112AF . 50 push eax
000112B0 . 68 A4820100 push 000182A4
000112B5 . E8 46FDFFFF call 00011000
000112BA . EB 08 jmp short 000112C4
000112BC > 6A 00 push 0
000112BE . FF15 8CAB0101 call dword ptr [&USER32.PostQuitMessage] PostQuitMessage
000112C4 > 31C0 xor eax, eax
000112C6 . EB 0D jmp short 000112D5

Call Stack:
Switch (cases 1..10)
Case 10 of switch 0001127F: DestroyWindow
Case 1 of switch 0001127F: ASCII "c:\windows\system32\notepad.exe"
Case 2 of switch 0001127F: ExitCode = 0; PostQuitMessage
Default case of switch 0001127F: DefWindowProcA

CPU Registers:
EAX: 00000000
ECX: 00000000
EDI: 00000000
ESI: 00000000

拦截到恶意木马

该恶意木马会对您的电脑进行恶意破坏

病毒名称：Win32.Trojan-Ransom.WannaCry.Y2.zav

病毒文件： 复件 wannasister.exe

文件路径：C:\Documents and Settings\PC\桌面

信任

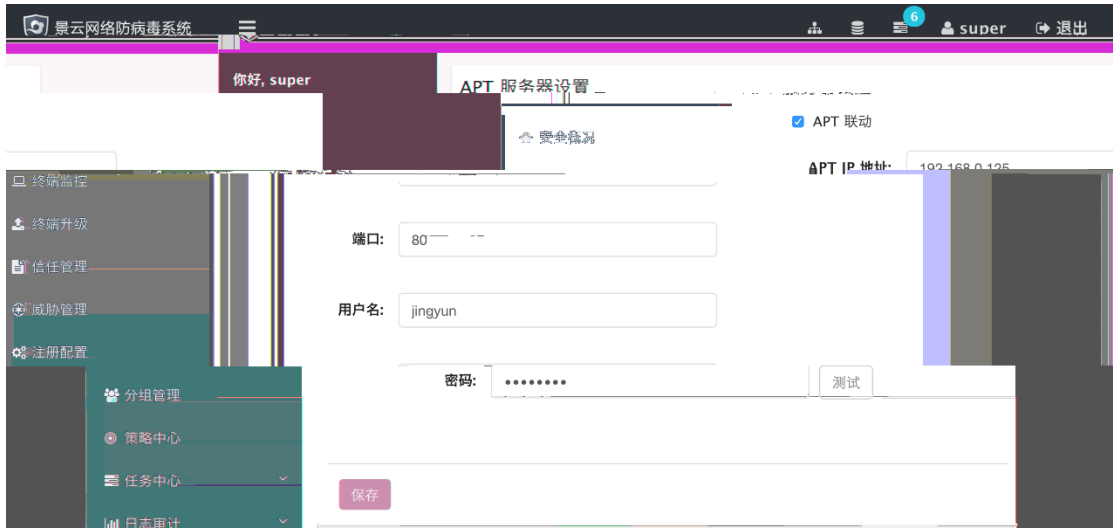
立即清除

The screenshot shows the main interface of the Jingyun Antivirus software. At the top, a notification bar indicates that 1 threat has been discovered. Below this, a table lists the detected threat. The sidebar on the right contains several menu items, some of which are checked.

类型	风险信息	处理建议
木马	Win32.Trojan-Ransom.WannaCry.Y2.zav C:\Documents and Settings\PC\桌面\wannasister.exe	建议删除

Sidebar menu items:

- 病毒查杀 风险扫描
- 实时防护 恶意木马
- 常用工具
- 防护日志
- 信任与隔离



文件信息

文件名 wannasister
文件类型 exe
文件大小 4.5 MB
扫描时间 2017-05-17 10:17:46
MD5 [REDACTED]
SHA1 [REDACTED]
SHA256 [REDACTED]

引擎

攻击类型 反调试
详细信息 尝试检测调试器
危险等级 ★★★★★

系统检测

操作系统: Windows XP SP3
软件版本: Adobe Reader 11
开始时间: 2017-05-17 10:17:59
结束时间: 2017-05-17 10:21:32

勒索软件 [1]

疑似勒索软件大量文件篡改行为 危险等级 ★★★★★

notepad.exe的勒索行为报警

ID	进程名	详细信息
36	C:\WINDOWS\system32\notepad.exe	file_modifications: Performs 245 file moves indicative of a potential file encryption process
36	C:\WINDOWS\system32\notepad.exe	appends_new_extension: Appends a new file extension to multiple modified files
36	C:\WINDOWS\system32\notepad.exe	new_appended_file_extension: .WNCRY
36	C:\WINDOWS\system32\notepad.exe	new_appended_file_extension: .WNCRYT

进程入侵 [4]

向其他进程写入可疑内容,试图将该进程作为傀儡进程启动 危险等级 ★★★★★

尝试打开系统进程中的线程 危险等级 ★★★★★

尝试创建傀儡进程 危险等级 ★★★

勒索模块代码被注入到notepad.exe中

进程名	详细信息
C:\Documents and Settings\Administrator\Local Settings\Temp\wannasister.exe	ProcessName: \Device\HarddiskVolume1\WINDOWS\system32\notepad.exe

虚拟机 [1]

开发 [1]

测试 [1]

调试 [1]

尝试检测调试器 危险等级 ★★★★★

威胁行为 [9]

检测码

流行度

动作

PID

1092

反虑

高并

反松

反调

尝试

威胁

VenusEye

Hedwig

Locky

18

Sage 2.0

Office

0day

2016

