

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	retn		

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	. 0740 00	mov	word ptr [ebp-00], eax
00011308	. 8D45 9C	lea	eax, dword ptr [ebp-64]
0001130B	. 50	push	eax
0001130C	. FF15 9CAB010	call	dword ptr [&USER32.RegisterClassEx]
0001130E	. 66:85C0	test	ax, ax
0001130F	. 74 75	je	short 0001143C
00011311	. 6A 00	push	0
00011313	. 56	push	esi
00011315	. 6A 00	push	0
00011317	. 6A 00	push	0
00011319	. 6A 78	push	78
0001131B	. 68 F0000000	push	0F0

RegisterClassEx

lpParam = NULL  
hInst = NULL  
hMenu = NULL  
hParent = NULL  
Height = 78 (120.)  
Width = F0 (240.)

0001131C	. 50	push	eax
0001131E	. 68 00020000	push	200
00011320	. FF15 A0AB010	call	dword ptr [&USER32.CreateWindowExA]
00011322	. 89C6	mov	esi, eax
00011324	. 85F6	test	esi, esi
00011326	. 74 9F	je	short 00011423
00011328	. 6A 00	push	0
0001132A	. 56	push	esi
0001132C	. FF15 A4AB010	call	dword ptr [&USER32.ShowWindow]
0001132E	. 56	push	esi
00011330	. FF15 A8AB010	call	dword ptr [&USER32.UpdateWindow]
00011332	. EB 14	jmp	short 00011423

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 88AB010	call	dword ptr [&USER32.DestroyWindow]
0001129A	. EB 28	jmp	short 000112C4
0001129C	. E8 AF010000	call	00011450
000112A1	. 6A 00	push	0
000112A3	. FF35 00A0010	push	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 8CAB010	call	dword ptr [&USER32.PostQuitMessage]
000112C4	. 31C0	xor	eax, eax
000112C6	. FR 0D	jmp	short 00011205

Switch (cases 1..10)

hWnd; Case 10 of switch 0001127F  
DestroyWindow

Case 1 of switch 0001127F

ASCII "c:\windows\system32\notepad.exe"

ExitCode = 0; Case 2 of switch 0001127F  
PostQuitMessage

default case of switch 0001127F

000112C7	. 57	push	edi
000112C8	. 56	push	esi
000112C9	. 53	push	ebx
000112CA	. FF15 90AB010	call	dword ptr [&USER32.DefWindowProc]
000112CC	. 57	pop	edi
000112CD	. 56	pop	esi
000112CE	. 53	pop	ebx



## 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

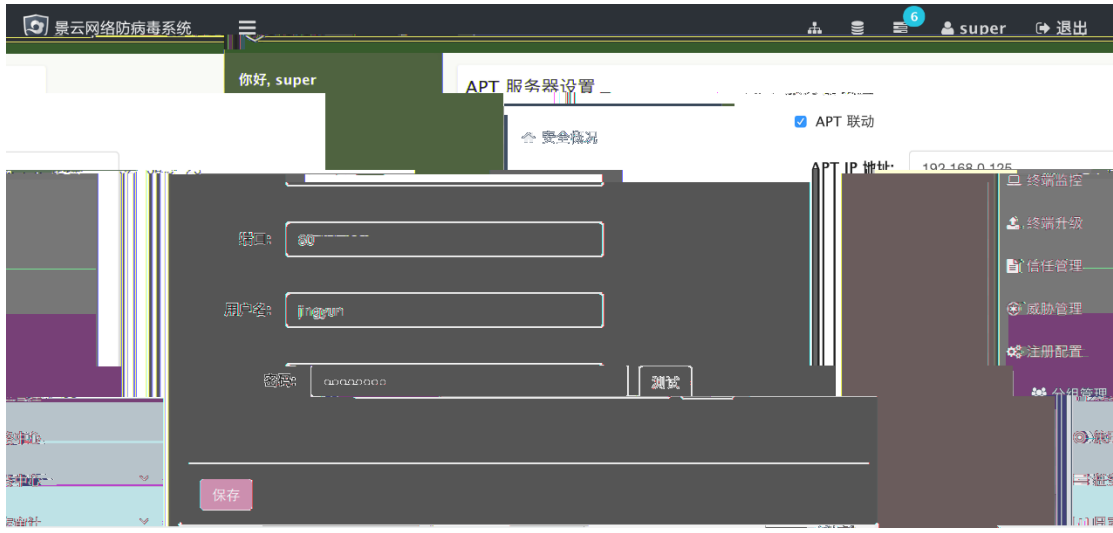
病毒文件： 复件 wannasister.exe

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, there is a title bar with the text '景云杀毒' and standard window controls. Below the title bar, there are two buttons: '不处理' (Do not process) and '立刻处理' (Process immediately). The main area displays the detected threat information, including the virus name 'Win32.Trojan-Ransom.WannaCry.Y2.zav' and the file path 'C:\Documents and Settings\PC\桌面\wannasister.exe'. A sidebar menu is open, showing options like '病毒查杀' (Virus scan), '实时防护' (Real-time protection), '常用工具' (Common tools), '防护日志' (Protection log), and '信任与隔离' (Trust and isolation). The '实时防护' option is currently selected. On the right side of the interface, there are checkboxes for '风险类型' (Risk type) and '恶意木马' (Malicious Trojan), both of which are checked. The '恶意木马' checkbox is highlighted with a red background. The risk information section shows 'Win32.Trojan-Ransom.WannaCry.Y2.zav' as the detected threat.



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]

静态检测

危险等级 ★★★☆☆ 检测引擎 流行威胁库 攻击类型 反调试 详细信息 尝试检测调试器

动态检测

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 10:21:3

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

PID	进程名	详细信息
996	C:\WINDOWS\system32\notepad.exe	file_modifications: Performs 245 file moves indicative of a potenti
996	C:\WINDOWS\system32\notepad.exe	_appends_new_extension: Appends a new file extension to multipl
996	C:\WINDOWS\system32\notepad.exe	new_appended_file_extension: .WNCRY
996	C:\WINDOWS\system32\notepad.exe	new_appended_file_extension: .WNCRYT

勒索行为报警

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 ★★★★★

勒索模块代码被注入到notepad.exe中

ProcessName: \Device\HarddiskVolume1\WINDOWS\system32\notepad.exe

危险等级 ★★★★★

- 反虚拟机 [1]
- 高并发 [1]
- 反检测 [1]
- 反调试 [1]
- 尝试检测调试器
- 可疑行为 [1]

VenusEye

Hedwig

Locky

18

Sage 2.0

Office

0day

2016

