

AAA:1000	95	push	ebp	
00011CD1	- 89E5	mov	ebp, esp	
00011CD3	- 83EC 04	sub	esp, 4	
00011CD6	- 53	push	ebx	
00011CD7	- 68 D9820100	push	000182D9	pModule = "ntdll.dll"
00011CDC	- FF15 B8A010	call	dword ptr [&KERNEL32.GetModuleHandleA	GetModuleHandleA
00011CE2	- 68 32820100	push	00018232	ProcNameOrOrdinal = "NtQueryInformationProcess"
00011CE7	- 50	push	eax	hModule
00011CE8	- FF15 BCA010	call	dword ptr [&KERNEL32.GetProcAddress	GetProcAddress

00011CF7	- 6A 0A	push	0	
00011CF8	- 6A 0A	push	4	
00011D01	- 8D55 FC	lea	edx, dword ptr [ebp-4]	
00011D04	- 52	push	edx	
00011D05	- 6A 07	push	7	
00011D07	- 50	push	eax	
00011D08	- FFDB	call	ebx	
00011D0A	- 837D FC 00	cmp	dword ptr [ebp-4], 0	

00011D12	- E8 D98000	call	dword ptr [ebp-4]	
00011D17	- 5B	pop	ebx	
00011D18	- 89EC	mov	esp, ebp	
00011D1A	- 5D	pop	ebp	
00011D1B	- C3	retn		
00011D1C	- 8D7C27 00	lea	edi, dword ptr [edi]	

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	. 0745 00	mov	dword ptr [ebp-00], eax
00011308	. 8D45 9C	lea	eax, dword ptr [ebp-64]
0001130B	. 50	push	eax
0001130C	. FF15 9CAB010	call	dword ptr [&USER32.RegisterClassExA]
0001130E	. 66:85C0	test	ax, ax
0001130F	. 74 75	je	short 0001143C
00011310	. 6A 00	push	0
00011311	. 56	push	esi
00011312	. 6A 00	push	0
00011313	. 6A 00	push	0
00011314	. 6A 78	push	78
00011315	. 68 F0000000	push	0F0

hWndClassEx
 RegisterClassExA
 lParam = NULL
 hInst
 hMenu = NULL
 hParent = NULL
 Height = 78 (120.)
 Width = F0 (240.)

00011316	. 68 0000CF00	lea	eax, dword ptr [ebp-16]
00011317	. 8D45 EA	lea	eax, dword ptr [ebp-16]
00011318	. 50	push	eax
00011319	. 0745 00	mov	dword ptr [ebp-00], eax
0001131A	. 68 00020000	push	eax
0001131B	. FF15 A0AB010	call	dword ptr [&USER32.CreateWindowExA]
0001131C	. 89C6	mov	esi, eax
0001131D	. 85F6	test	esi, esi
0001131E	. 74 3F	je	short 0001143C
0001131F	. 6A 00	push	0
00011320	. 56	push	esi
00011321	. FF15 A4AB010	call	dword ptr [&USER32.ShowWindow]
00011322	. 56	push	esi
00011323	. FF15 A8AB010	call	dword ptr [&USER32.UpdateWindow]
00011324	. EB 14	jmp	short 00011423

WS_EX_CLIENTEDGE
 CreateWindowExA
 SW_HIDE
 ShowWindow
 UpdateWindow

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 00	jmp	short 0001129C

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	. FF7424 1C	lea	edi, dword ptr [esp+1C]
00011280	. 57	push	edi
00011281	. 56	push	esi
00011282	. 53	push	ebx
00011283	. FF15 90AB010	call	dword ptr [&USER32.DefWindowProcA]
00011285	. 5F	push	edi
00011286	. 5E	push	esi
00011287	. FR 00	jmp	short 0001129C

wParam
 message
 hWnd
 DefWindowProcA

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 displays the Jingyun Antivirus (景云杀毒) interface. At the top, a notification banner reads "发现 1 个威胁" (Found 1 threat) with buttons for "暂不处理" (Do not process) and "立刻处理" (Process immediately). Below this, a table lists the detected threat:

病毒名称	处理建议
Win32.Trojan-Ransom.WannaCry.Y2.zav	建议删除
C:\Documents and Settings\PC\桌面\wannasister.exe	

On the right side, a sidebar menu includes 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 logs), and "信任与隔离" (Trust and isolation). A "自定义杀毒已完成" (Custom virus scan completed) notification is visible at the top right. The main area on the right shows a list of threat details:

风险类型	风险信息
<input checked="" type="checkbox"/> 恶意木马	Win32.Trojan-Ransom.WannaCry.Y2.zav C:\Documents and Settings\PC\桌面\wannasister.exe

你好, super

APT 服务器设置

安全策略

APT 联动

APT IP 地址: 192.168.0.125

端口: 80

用户名: jingyun

密码:

- 终端升级
- 信任管理
- 威胁管理
- 注册配置
- 分组管理
- 策略中心
- 任务中心
- 日志统计

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

检测引擎: 病毒引擎: 引擎规则: 引擎版本:
运行策略: 反病毒: 完整检测策略: ☆☆☆☆☆

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 10:21:32

静态软件 [1]

PID	进程名	详细信息
496	CAWINDOWS\system32\notepad.exe	file_modifications: Performs 245 file moves indicative of a potential file encryption p
496	CAWINDOWS\system32\notepad.exe	appends_new_extension: Appends a new file extension to multiple modified files:
496	CAWINDOWS\system32\notepad.exe	new_appended_file_extension: .WNCRY
496	CAWINDOWS\system32\notepad.exe	new_appended_file_extension: .WNCRY

进程入侵 [1]

- 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

:\HarddiskVolume1\WINDOWS\system32\notepad.exe

PID	进程名	详细信息
1092	C:\Documents and Settings\svAdministrator\Local Settings\Temp\wannasister.exe	ProcessName: \Device

- 反虚拟机 [1]
- 高并发 [1]
- 反检测 [1]
- 反调试 [1]
- 尝试检测调试器 危险等级 ☆☆☆☆☆
- 威胁行为 [9]

VenusEye

Hedwig

Locky

18

Sage 2.0

Office

0day

2016

