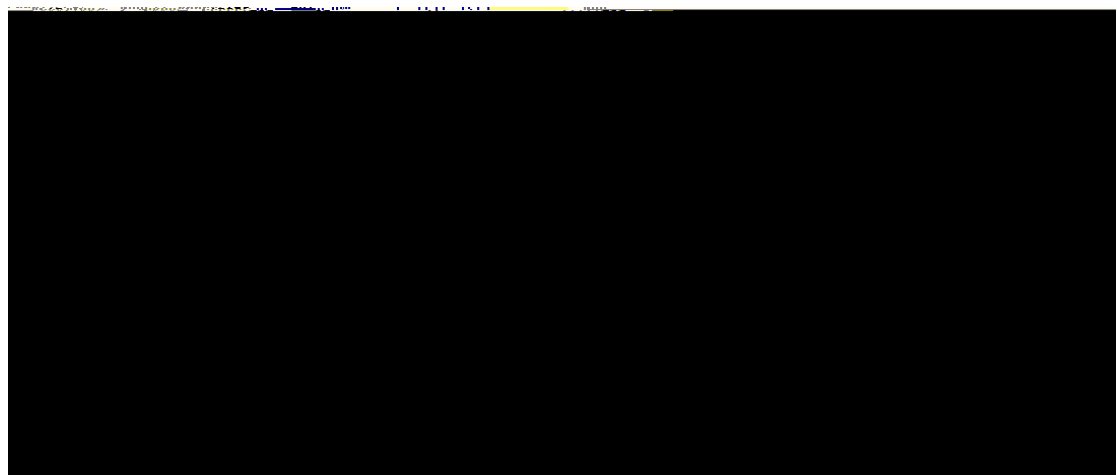




00011C80	\$ 55	push	ebp	
00011C81	. 89E5	mov	ebp, esp	
00011C83	. 83EC 04	sub	esp, 4	
00011C86	. 64:A1 300000	mov	eax, dword ptr fs:[30]	
00011C8C	. 8B40 68	mov	eax, dword ptr [eax+68]	
00011C8F	. 8945 FC	mov	dword ptr [ebp-4], eax	
00011C92	. 8B45 FC	mov	eax, dword ptr [ebp-4]	
00011C95	. 89EC	mov	esp, 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 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.RegisterClassEx]	RegisterClassEx
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	
00011316	. 50	push	0	
00011317	. 50	push	0	
00011318	. 50	push	0	
00011319	. 50	push	0	
0001131A	. 50	push	0	
0001131B	. 50	push	0	
0001131C	. 50	push	0	
0001131D	. 50	push	0	
0001131E	. 50	push	0	
0001131F	. 50	push	0	
00011320	. 50	push	0	
00011321	. 50	push	0	
00011322	. 50	push	0	
00011323	. 50	push	0	
00011324	. 50	push	0	
00011325	. 50	push	0	
00011326	. 50	push	0	
00011327	. 50	push	0	
00011328	. 50	push	0	
00011329	. 50	push	0	
0001132A	. 50	push	0	
0001132B	. 50	push	0	
0001132C	. 50	push	0	
0001132D	. 50	push	0	
0001132E	. 50	push	0	
0001132F	. 50	push	0	
00011330	. 50	push	0	
00011331	. 50	push	0	
00011332	. 50	push	0	
00011333	. 50	push	0	
00011334	. 50	push	0	
00011335	. 50	push	0	
00011336	. 50	push	0	
00011337	. 50	push	0	
00011338	. 50	push	0	
00011339	. 50	push	0	
0001133A	. 50	push	0	
0001133B	. 50	push	0	
0001133C	. 50	push	0	
0001133D	. 50	push	0	
0001133E	. 50	push	0	
0001133F	. 50	push	0	
00011340	. 50	push	0	
00011341	. 50	push	0	
00011342	. 50	push	0	
00011343	. 50	push	0	
00011344	. 50	push	0	
00011345	. 50	push	0	
00011346	. 50	push	0	
00011347	. 50	push	0	
00011348	. 50	push	0	
00011349	. 50	push	0	
0001134A	. 50	push	0	
0001134B	. 50	push	0	
0001134C	. 50	push	0	
0001134D	. 50	push	0	
0001134E	. 50	push	0	
0001134F	. 50	push	0	
00011350	. 50	push	0	
00011351	. 50	push	0	
00011352	. 50	push	0	
00011353	. 50	push	0	
00011354	. 50	push	0	
00011355	. 50	push	0	
00011356	. 50	push	0	
00011357	. 50	push	0	
00011358	. 50	push	0	
00011359	. 50	push	0	
0001135A	. 50	push	0	
0001135B	. 50	push	0	
0001135C	. 50	push	0	
0001135D	. 50	push	0	
0001135E	. 50	push	0	
0001135F	. 50	push	0	
00011360	. 50	push	0	
00011361	. 50	push	0	
00011362	. 50	push	0	
00011363	. 50	push	0	
00011364	. 50	push	0	
00011365	. 50	push	0	
00011366	. 50	push	0	
00011367	. 50	push	0	
00011368	. 50	push	0	
00011369	. 50	push	0	
0001136A	. 50	push	0	
0001136B	. 50	push	0	
0001136C	. 50	push	0	
0001136D	. 50	push	0	
0001136E	. 50	push	0	
0001136F	. 50	push	0	
00011370	. 50	push	0	
00011371	. 50	push	0	
00011372	. 50	push	0	
00011373	. 50	push	0	
00011374	. 50	push	0	
00011375	. 50	push	0	
00011376	. 50	push	0	
00011377	. 50	push	0	
00011378	. 50	push	0	
00011379	. 50	push	0	
0001137A	. 50	push	0	
0001137B	. 50	push	0	
0001137C	. 50	push	0	
0001137D	. 50	push	0	
0001137E	. 50	push	0	
0001137F	. 50	push	0	
00011380	. 50	push	0	
00011381	. 50	push	0	
00011382	. 50	push	0	
00011383	. 50	push	0	
00011384	. 50	push	0	
00011385	. 50	push	0	
00011386	. 50	push	0	
00011387	. 50	push	0	
00011388	. 50	push	0	
00011389	. 50	push	0	
0001138A	. 50	push	0	
0001138B	. 50	push	0	
0001138C	. 50	push	0	
0001138D	. 50	push	0	
0001138E	. 50	push	0	
0001138F	. 50	push	0	
00011390	. 50	push	0	
00011391	. 50	push	0	
00011392	. 50	push	0	
00011393	. 50	push	0	
00011394	. 50	push	0	
00011395	. 50	push	0	
00011396	. 50	push	0	
00011397	. 50	push	0	
00011398	. 50	push	0	
00011399	. 50	push	0	
0001139A	. 50	push	0	
0001139B	. 50	push	0	
0001139C	. 50	push	0	
0001139D	. 50	push	0	
0001139E	. 50	push	0	
0001139F	. 50	push	0	
000113A0	. 50	push	0	
000113A1	. 50	push	0	
000113A2	. 50	push	0	
000113A3	. 50	push	0	
000113A4	. 50	push	0	
000113A5	. 50	push	0	
000113A6	. 50	push	0	
000113A7	. 50	push	0	
000113A8	. 50	push	0	
000113A9	. 50	push	0	
000113AA	. 50	push	0	
000113AB	. 50	push	0	
000113AC	. 50	push	0	
000113AD	. 50	push	0	
000113AE	. 50	push	0	
000113AF	. 50	push	0	
000113B0	. 50	push	0	
000113B1	. 50	push	0	
000113B2	. 50	push	0	
000113B3	. 50	push	0	
000113B4	. 50	push	0	
000113B5	. 50	push	0	
000113B6	. 50	push	0	
000113B7	. 50	push	0	
000113B8	. 50	push	0	
000113B9	. 50	push	0	
000113BA	. 50	push	0	
000113BB	. 50	push	0	
000113BC	. 50	push	0	
000113BD	. 50	push	0	
000113BE	. 50	push	0	
000113BF	. 50	push	0	
000113C0	. 50	push	0	
000113C1	. 50	push	0	
000113C2	. 50	push	0	
000113C3	. 50	push	0	
000113C4	. 50	push	0	
000113C5	. 50	push	0	
000113C6	. 50	push	0	
000113C7	. 50	push	0	
000113C8	. 50	push	0	
000113C9	. 50	push	0	
000113CA	. 50	push	0	
000113CB	. 50	push	0	
000113CC	. 50	push	0	
000113CD	. 50	push	0	
000113CE	. 50	push	0	
000113CF	. 50	push	0	
000113D0	. 50	push	0	
000113D1	. 50	push	0	
000113D2	. 50	push	0	
000113D3	. 50	push	0	
000113D4	. 50	push	0	
000113D5	. 50	push	0	
000113D6	. 50	push	0	
000113D7	. 50	push	0	
000113D8	. 50	push	0	
000113D9	. 50	push	0	
000113DA	. 50	push	0	
000113DB	. 50	push	0	
000113DC	. 50	push	0	
000113DD	. 50	push	0	
000113DE	. 50	push	0	
000113DF	. 50	push	0	
000113E0	. 50	push	0	
000113E1	. 50	push	0	
000113E2	. 50	push	0	
000113E3	. 50	push	0	
000113E4	. 50	push	0	
000113E5	. 50	push	0	
000113E6	. 50	push	0	
000113E7	. 50	push	0	
000113E8	. 50	push	0	
000113E9	. 50	push	0	
000113EA	. 50	push	0	
000113EB	. 50	push	0	
000113EC	. 50	push	0	
000113ED	. 50	push	0	
000113EE	. 50	push	0	
000113EF	. 50	push	0	
000113F0	. 50	push	0	
000113F1	. 50	push	0	
000113F2	. 50	push	0	
000113F3	. 50	push	0	
000113F4	. 50	push	0	
000113F5	. 50	push	0	
000113F6	. 50	push	0	
000113F7	. 50	push	0	
000113F8	. 50	push	0	
000113F9	. 50	push	0	
000113FA	. 50	push	0	
000113FB	. 50	push	0	
000113FC	. 50	push	0	
000113FD	. 50	push	0	
000113FE	. 50	push	0	
000113FF	. 50	push	0	

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	Switch (cases 1..10)
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	hWnd; Case 10 of switch 0001127F
00011294	. FF15 88AB010	call	dword ptr [<&USER32.DestroyWindow]	DestroyWindow
0001129A	. EB 28	jmp	short 000112C4	
0001129C	> E8 AF010000	call	00011450	Case 1 of switch 0001127F
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	ASCII "c:\windows\system32\notepad.exe"
000112B5	. E8 46FDFFFF	call	00011000	
000112BA	. EB 08	jmp	short 000112C4	
000112BC	> 6A 00	push	0	ExitCode = 0; Case 2 of switch 0001127F
000112BE	. FF15 8CAB010	call	dword ptr [<&USER32.PostQuitMessage]	PostQuitMessage
000112C4	> 31C0	xor	eax, eax	
000112C6	. ER 00	jmp	short 000112D5	
000112C8	. 5B	pop	ebx	
000112C9	. 5E	pop	esi	
000112CA	. 5F	pop	edi	
000112CB	. 58	pop	eax	
000112CC	. 59	pop	ecx	
000112CD	. 5A	pop	edx	
000112CE	. 5B	pop	ebx	
000112CF	. 5C	pop	esi	
000112D0	. 5D	pop	edi	
000112D1	. 5E	pop	esi	
000112D2	. 5F	pop	edi	
000112D3	. 58	pop	eax	
000112D4	. 59	pop	ecx	
000112D5	. 5A	pop	edx	
000112D6	. 5B	pop	ebx	
000112D7	. 5C	pop	esi	
000112D8	. 5D	pop	edi	
000112D9	. 5E	pop	esi	
000112DA	. 5F	pop	edi	
000112DB	. 58	pop	eax	
000112DC	. 59	pop	ecx	
000112DD	. 5A	pop	edx	
000112DE	. 5B	pop	ebx	
000112DF	. 5C	pop	esi	
000112E0	. 5D	pop	edi	
000112E1	. 5E	pop	esi	
000112E2	. 5F	pop	edi	
000112E3	. 58	pop	eax	
000112E4	. 59	pop	ecx	
000112E5	. 5A	pop	edx	
000112E6	. 5B	pop	ebx	
000112E7	. 5C	pop	esi	
000112E8	. 5D	pop	edi	
000112E9	. 5E	pop	esi	
000112EA	. 5F	pop	edi	
000112EB	. 58	pop	eax	
000112EC	. 59	pop	ecx	
000112ED	. 5A	pop	edx	
000112EE	. 5B	pop	ebx	
000112EF	. 5C	pop	esi	
000112F0	. 5D	pop	edi	
000112F1	. 5E	pop	esi	
000112F2	. 5F	pop	edi	
000112F3	. 58	pop	eax	
000112F4	. 59	pop	ecx	
000112F5	. 5A	pop	edx	
000112F6	. 5B	pop	ebx	
000112F7	. 5C	pop	esi	
000112F8	. 5D	pop	edi	
000112F9	. 5E	pop	esi	
000112FA	. 5F	pop	edi	
000112FB	. 58	pop	eax	
000112FC	. 59	pop	ecx	
000112FD	. 5A	pop	edx	
000112FE	. 5B	pop	ebx	
000112FF	. 5C	pop	esi	

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

景云杀毒



病毒查杀

实时防护

常用工具

防护日志

信任与隔离

发现 1 个威胁

自定义查杀已完成。耗时 00:07，扫描项目 1 个

暂时不处理 立刻处理

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



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

SHA1 

SHA256

諸君共鑒

[详细信息](#)

尝试检测调试器

危險等級

★★★★☆

检测引擎

流行威胁库

攻击类型

反调试

动态检测

操作系统： Windows XP SP3

开始时间： 2017-05-17 10:17:59

- 勒索软件 [1]

疑似勒索软件大量文件篡改行为 危险等级 1

PID	进程名	详
996	C:\WINDOWS\system32\notepad.exe	fil
996	C:\WINDOWS\system32\notepad.exe	aj
996	C:\WINDOWS\system32\notepad.exe	ru
996	C:\WINDOWS\system32\notepad.exe	ru

- 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

▶ 尝试打开系统进程中的线程 危险等级 ★★

★★★★★

notepad.exe的勒索行为报警

[详细信息](#)

le_modifications: Performs 245 file moves indicative of a potential file encryption process

`opens_new_extension`: Appends a new file extension to multiple modified files

```
ew_appended_file_extension: .WNCRY
```

```
new_appended_file_extension: .WNCRYT
```

⚠️ 进程启动 危险等级 ★★★★★

☆☆☆

危險等級 ★★★

[illegible]

VenusEye

VenusEye

Hedwig

Locky

18

Sage 2.0

Office

0day

2016

