

勒索病毒“wannacry”升级新变种“wannasister”

2017年5月16日，金睛安全研究团队监控到了席卷全球的“wannacry”勒索病毒出现了一个最新变种，名为“wannasister”。该变种增加了一些反调试功能，同时将主要的勒索模块代码注入到正常的记事本（notepad.exe）进程中，并且其中用于加密 AES 密钥的内置 RSA 公钥也与之前的版本有了变化。种种迹象显示，勒索病毒有可能在短期内出现第二波攻势，用户需高度警惕。

技术分析

1. 新变种在运行之初增加了一些反调试的功能。

(1) 通过检测 DebugPort 来检测调试器是否存在。

```
00011CD0 55 push ebp
00011CD1 89E5 mov ebp, esp
00011CD3 83EC 04 sub esp, 4
00011CD6 5B push ebx
00011CD7 68 D9820100 push 000182D9
00011CDC FF15 B8A00100 call dword ptr [ &KERNEL32.GetModuleHandleA
00011CE2 68 32820100 push 00018232
00011CE7 50 push eax
00011CE8 FF15 BCAA0100 call dword ptr [ &KERNEL32.GetProcAddress
00011CEE 89C3 mov ebx, eax
00011CF0 C745 FC 0000 mov dword ptr [ebp-4], 0
00011CF7 FF15 ECA00100 call dword ptr [ &KERNEL32.GetCurrentProcess
00011CFD 6A 00 push 0
00011CFF 6A 04 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 FFD3 call ebx
00011D0A 837D FC 00 cmp dword ptr [ebp-4], 0
00011D0E 74 07 ja short 00011D17
00011D10 6A 00 push 0
00011D12 E8 D98D0000 call <&KERNEL32.ExitProcess>
00011D17 5B pop ebx
00011D18 89EC mov esp, ebp
00011D1A 5D pop ebp
00011D1B C3 retn
00011D1C 8D7C27 00 lea edi, dword ptr [edi]
00011D20 EC retn
```

(2) 通过检测 NtGlobalFlag 来检测调试器是否存在。

```
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
```

(3) 如果检测出调试器则直接构造异常。

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

2.新变种的主要功能函数写在了窗口回调函数中，手法更加隐蔽

(1) 通过 RegisterClassExA 注册窗口回调

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>] 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
00011316	. 68 00000000	push	80000000
00011317	. 68 00000000	push	80000000
00011318	. 68 0000CF00	push	0CF0000
00011319	. 8D45 EA	lea	eax, dword ptr [ebp-16]
0001131A	. 50	push	eax
0001131B	. 8D45 F3	lea	eax, dword ptr [ebp-D]
0001131C	. 50	push	eax
0001131D	. 68 00020000	push	200
0001131E	. FF15 A0AB010	call	dword ptr [<USER32.CreateWindowExA>] CreateWindowExA
0001131F	. 89C6	mov	esi, eax
00011320	. 85F6	test	esi, esi
00011321	.. 74 3F	je	short 0001143C
00011322	. 6A 00	push	0
00011323	. 56	push	esi
00011324	. FF15 A4AB010	call	dword ptr [<USER32.ShowWindow>] ShowWindow
00011325	. 56	push	esi
00011326	. FF15 A8AB010	call	dword ptr [<USER32.UpdateWindow>] UpdateWindow
00011327	.. EB 14	jmp	short 00011423

(2)主要的窗口回调函数

00011270	. 53	push	ebx
00011271	. 56	push	esi
00011272	. 57	push	edi
00011273	. 8B5C24 10	mov	ebx, dword ptr [esp+10]
00011274	. 8B7424 14	mov	esi, dword ptr [esp+14]
00011275	. 8B7C24 18	mov	edi, dword ptr [esp+18]
00011276	. 83FE 01	cmp	esi, 1
00011277	.. 74 18	je	short 0001129C
00011278	. 83FE 02	cmp	esi, 2
00011279	.. 74 33	je	short 000112BC
0001127A	. 83FE 01	cmp	esi, 1
0001127B	.. 7C 3A	jl	short 000112C8
0001127C	. 83FE 10	cmp	esi, 10
0001127D	.. 75 35	jnz	short 000112C8
0001127E	. 53	push	ebx
0001127F	. FF15 88AB010	call	dword ptr [<USER32.DestroyWindow>] DestroyWindow
00011280	.. EB 28	jmp	short 000112C4
00011281	> E8 AF010000	call	00011450
00011282	. 6A 00	push	0
00011283	. FF35 00A0010	push	dword ptr [1A000]
00011284	. 50	push	eax
00011285	. E8 11020000	call	000114C0
00011286	. 50	push	eax
00011287	. 68 A4820100	push	000182A4
00011288	. E8 46FDFFFF	call	00011000
00011289	.. EB 08	jmp	short 000112C4
0001128A	> 6A 00	push	0
0001128B	> FF15 8CAB010	call	dword ptr [<USER32.PostQuitMessage>] PostQuitMessage
0001128C	> 31C0	xor	eax, eax
0001128D	.. EB 0D	jmp	short 000112D5
0001128E	> FF7424 1C	push	dword ptr [esp+1C]
0001128F	. 57	push	edi
00011290	. 56	push	esi
00011291	. 53	push	ebx
00011292	. FF15 90AB010	call	dword ptr [<USER32.DefWindowProcA>] DefWindowProcA
00011293	> 5F	pop	edi
00011294	. 5E	pop	esi
00011295	. 5B	pop	ebx

3.新变种的主要勒索功能采用了注入正常记事本进程（notepad.exe）进程的方式。这样做是

为了躲避一些杀软主动防御功能,甚至可能会绕过一些软件的勒索保护功能,潜在危害更大。因为某些具有勒索保护功能的主动防御类软件是默认放过 notepad.exe,winword.exe 等文字编辑工具修改文档文件的。

```

000111AB . 8345 F8      add     eax, dword ptr [ebp-8]
000111AE . 50          push   eax
000111AF . FF75 E4     push   dword ptr [ebp-1C]
000111B2 . FF15 C4AA0101 call   dword ptr [<&KERNEL32.WriteProcessMemory
000111B8 . 85C0       test   eax, eax
000111BA . 0F84 00FFFFF je     000110C0
000111C0 . 8B46 10     mov     eax, dword ptr [esi+10]
000111C3 . 3B45 FC     cmp     eax, dword ptr [ebp-4]
000111C6 . 0F85 F4FEFFF jnz    000110C0
000111CC > 47         inc     edi
000111CD . 83C6 28     add     esi, 28
000111D0 > 0FB743 06   movzx  eax, word ptr [ebx+6]
000111D4 . 39C7       cmp     edi, eax
000111D6 . 7C BC     jl     short 00011194
000111D8 . 8D45 FC     lea    eax, dword ptr [ebp-4]
000111DB . 50          push   eax
000111DC . 6A 04     push   4
000111DE . 8D45 F8     lea    eax, dword ptr [ebp-8]
000111E1 . 50          push   eax
000111E2 . 8B85 78DFFFF mov     eax, dword ptr [ebp-288]
000111E8 . 83C0 08     add     eax, 8
000111EB . 50          push   eax
000111EC . FF75 E4     push   dword ptr [ebp-1C]
000111EF . FF15 C4AA0101 call   dword ptr [<&KERNEL32.WriteProcessMemory
000111F5 . 85C0       test   eax, eax
000111F7 . 0F84 C3FEFFF je     000110C0
000111FD . 837D FC 04   cmp     dword ptr [ebp-4], 4
00011201 . 0F85 B9FEFFF jnz    000110C0
00011207 . 8B5B 28     mov     ebx, dword ptr [ebx+28]
0001120A . 835D F8     add     ebx, dword ptr [ebp-8]
0001120D . 899D 84DFFFF mov     dword ptr [ebp-27C], ebx
00011213 . 8D85 D4FCFFF lea    eax, dword ptr [ebp-32C]
00011219 . 50          push   eax
0001121A . FF75 E8     push   dword ptr [ebp-18]
0001121D . FF15 C8AA0101 call   dword ptr [<&KERNEL32.SetThreadContext
00011223 . FF75 E8     push   dword ptr [ebp-18]
00011226 . FF15 CCAA0101 call   dword ptr [<&KERNEL32.ResumeThread

```

4.notepad.exe 中被注入的代码为和 wannacry 勒索病毒释放的勒索主程序 tasksche.exe 完全相同。但其内嵌的用来加密 AES 密钥的 RSA 公钥出现了变化。

Hex	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
CF40h:	06	02	00	00	00	A4	00	00	52	53	41	31	00	08	00	00w..RSA1....
CF50h:	01	00	01	00	75	97	4C	3B	84	46	DE	2C	2A	F4	95	A8u-L;„FB,*ó*
CF60h:	5D	C0	CD	6D	DA	D7	D4	92	1E	13	82	34	6A	70	8D	8F]ÄimÜ×Ö;„,4jp..
CF70h:	7C	F7	04	92	55	7F	F1	A2	27	B2	9E	41	AC	90	80	91	÷.'U.ñó'zA-.e'
CF80h:	18	93	C2	B1	7B	AD	2B	F3	FF	AF	DB	2B	51	BE	1D	A3	."Ä±(-+óýÜ+Q%..f
CF90h:	27	E3	A7	57	08	5A	BE	C1	1D	F6	04	F8	1C	BE	5B	B1	'ššW.2%Ä.š.š.%(±
CFA0h:	67	FB	E4	C8	DA	75	00	70	B1	17	70	24	6C	09	63	74	güÄëÜu.p.±\$1.ct
CFB0h:	AC	48	0A	1D	71	AE	7F	AE	65	B8	C5	86	79	C5	7E	9F	-K..qö.öe.ÄtyÄ-Y
CFC0h:	98	60	4C	52	B9	29	62	CB	23	29	ED	31	91	74	7B	7B	~IR'')bE#)i1t{(
CFD0h:	0B	26	1B	F2	7D	67	BF	DA	7A	40	DA	F2	61	4D	94	A5	.š.ó)gÜzÜöAM"¥
CFE0h:	7D	AD	59	6B	AD	9E	A3	3A	39	C6	5B	6E	9F	D2	BB	36]-Yk-šš:9E[nYöš6
CFE0h:	B5	F5	D2	65	F5	2C	30	D8	C1	17	BD	AF	28	00	96	20	ušöeš,00Ä.%(.-
D000h:	46	A7	2D	62	03	0C	D7	D0	75	A0	0B	07	EA	D4	1F	CA	Fš-b..×öu . .ëö.Ë
D010h:	E8	D9	4E	DB	38	F2	26	75	CB	12	A6	88	70	9B	E1	EA	ëÜNÜšöšöe. ;'p>šë
D020h:	32	DC	F8	71	72	50	41	E6	17	81	68	27	42	8E	DF	E5	2ÜšöqrPÄe..h'Bžšš
D030h:	DE	A1	72	D9	3B	FB	E5	9D	30	11	69	92	CD	60	2B	E2	B;rxÜ;šš.0.i'í'+š
D040h:	D5	46	3C	28	CF	9D	30	4A	F7	AD	B9	FB	0F	91	FE	2E	ÖF<(í.0J÷-šš. 'p.

newone

Hex	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
CF40h:	06	02	00	00	00	A4	00	00	52	53	41	31	00	08	00	00w..RSA1....
CF50h:	01	00	01	00	2F	A3	F1	6A	05	4E	44	4B	C7	D5	85	D8/ššj.NDKšö.š
CF60h:	F9	A4	A1	1B	79	F1	DA	73	48	94	18	FC	27	6B	EC	7B	ù*;yñÜšH".ü'ki{
CF70h:	98	0B	87	DB	5A	FA	7F	EB	79	6A	AF	A1	EC	78	BF	3B	~.+ÜZú.éyÿ;ixç;
CF80h:	5C	19	96	FA	2B	D4	AB	33	B9	CD	EF	00	2E	3A	69	EE	\.-ú+öš3'íi...:if
CF90h:	09	30	DC	DB	28	13	FB	9F	76	4D	B7	C9	48	4B	34	0A	.0ÜÜ(.šYvM-ËHK4.
CFA0h:	42	F5	F8	2F	AC	86	19	D9	6F	93	F6	B3	93	1A	C8	62	Böü/-+.Üö"šö".Èb
CFB0h:	9C	D9	13	9D	7C	7A	84	F5	58	43	05	E7	5C	41	11	92	æÜ.. z„šXC.ç\A.'
CFC0h:	E6	37	C8	8C	C7	41	4C	3C	82	03	D0	CA	A0	72	2B	83	æ7Ë@ÇAL<..šË r+f
CFD0h:	72	F8	CB	F5	32	79	E9	2B	66	5E	DC	B6	22	0F	92	91	røËšš2yé+f^ÜË".'
CFE0h:	A5	05	48	8C	93	6D	7F	F0	3B	4E	47	5E	E2	7C	68	D4	¥.HË"m.š;NG^š hö
CFE0h:	ED	67	39	57	CB	80	E2	01	26	DD	66	F9	23	05	38	42	íg9WËEéA.šYfúš.šB
D000h:	C9	41	0D	D2	A0	D9	36	8A	1A	21	2F	A2	BF	4B	19	73	EA.ö Üšš.!/çzK.s
D010h:	52	D5	85	30	09	C4	87	5B	49	FC	EF	97	57	27	3B	B5	Rö.0.Ä±[Iüi-W';µ
D020h:	43	AD	C1	00	2E	96	38	18	51	15	43	62	A2	3B	91	D9	C-Ä..-š.Q.Cbç;Ü
D030h:	5B	F7	62	A3	72	F1	10	7F	CC	2B	47	30	8B	74	3F	AF	[÷bšrñ..í+öçt?~
D040h:	3A	5D	B9	56	2E	9B	FA	89	02	41	25	09	3F	D0	83	72	:]V. >úš.Aš.šDfz

解决方案

1. 景云终端防病毒最新版本可彻底查杀“wannasister”病毒最新变种。

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. On the left is a dark sidebar with navigation options: 景云杀毒 (Jingyun Antivirus), 病毒查杀 (Virus Scanning), 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 main area has a dark header with the title '发现 1 个威胁' (Found 1 threat) and a status bar indicating '自定义查杀已完成, 耗时 00:07, 扫描项目 1 个' (Custom scan completed, 00:07, 1 item scanned). Below this is a table of detected threats.

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

- 即使未来再出现新的勒索病毒变种，也可使用景云杀毒与 APT 联动的方式，进行未知勒索病毒的检测与防护。

你好, super

🏠 安全概况

🖥️ 终端监控

👤 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

📄 日志审计

APT 服务器设置

APT 联动

APT IP 地址:

端口:

用户名:

密码:

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 攻击类型 详细信息 危险等级
流行威胁库 反调试 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 10:21:32

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

PID	进程名	详细信息
996	C:\WINDOWS\system32\notepad.exe	file_modifications: Performs 245 file moves indicative of a potential file encryption process
996	C:\WINDOWS\system32\notepad.exe	appends_new_extension: Appends a new file extension to multiple modified files
996	C:\WINDOWS\system32\notepad.exe	new_appended_file_extension: .WNCRYT
996	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 ★★★★★

尝试读取系统进程内存 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

PID	进程名	详细信息
1092	C:\Documents and Settings\sAdministrator\Local Settings\Temp\wannasister.exe	ProcessName: \Device\HarddiskVolume1\WINDOWS\system32\notepad.exe

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]

关于 VenusEye 金睛安全研究团队：

VenusEye 金睛安全研究团队是启明星辰集团检测产品本部从事专业安全分析的技术型团队，主要职责是对现有产品上报的安全事件、样本数据进行挖掘、分析，并向用户提供专业的分析报告。金睛团队会依据数据产生的威胁情报，对其中采用的各种攻击技术做深入的跟踪与分析，并给出专业分析结果、提出专业建议，为用户决策提供帮助。

金睛团队成立至今，先后发布了《小心，“宏”成为新攻击手法的主力军》、《海德薇 Hedwig 组织分析报告》、《Locky 密锁攻击恶意样本分析报告》、《特斯拉恶意样本分析新解》、《无需担心潜藏了 18 年的微软浏览器远程代码执行漏洞》、《鼠尾草 Sage 2.0 攻击样本信息通告》、《“凯莉”嵌套式攻击样本信息通告》、《Office 野外 0day 分析报告》、《2016 年度监测数据分析报告》等数十份专业安全分析报告，欢迎下载查阅。

