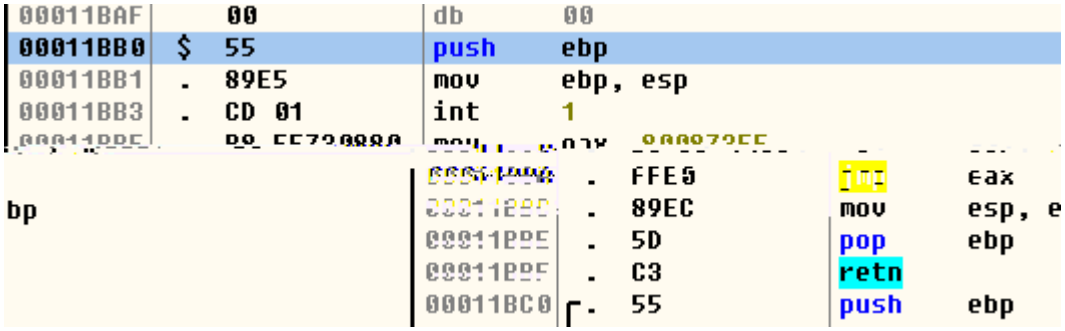
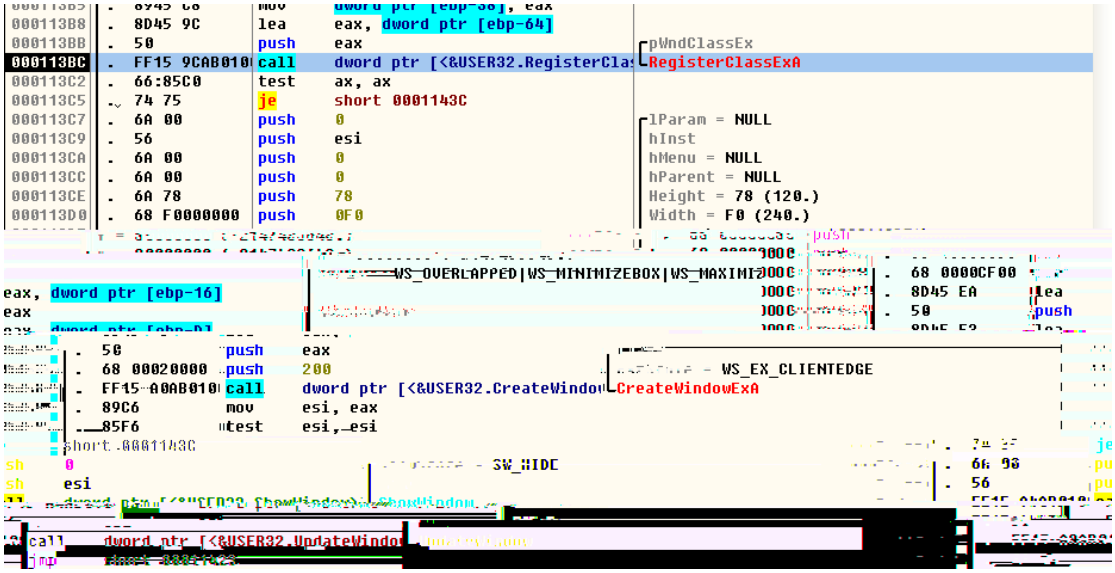
“ ” ”wannasister”

“ ”

“

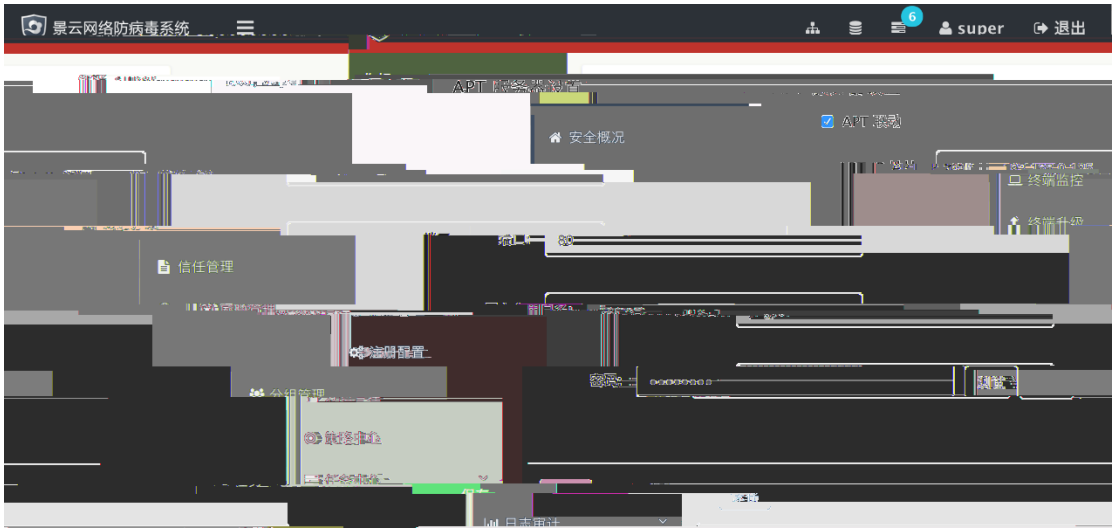
öJÕ

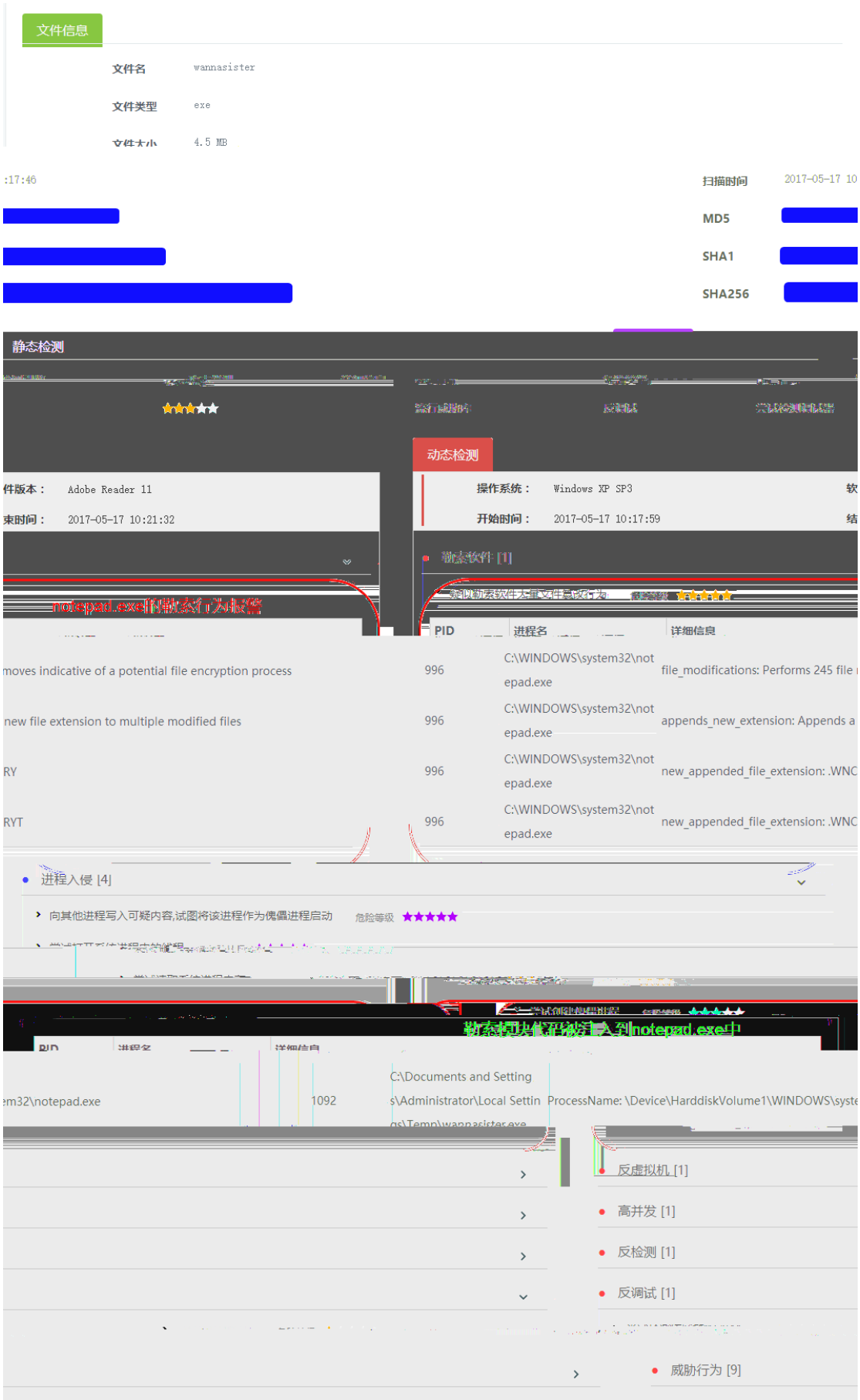

00011BAF 00 db 00
00011BB0 $ 55 push ebp
00011BB1 . 89E5 mov ebp, esp
00011BB3 . CD 01 int 1
. FFE0 jmp eax
. 89EC mov esp, e
. 5D pop ebp
. C3 retn
00011BC0 . 55 push ebp
bp


000113B8 . 8D45 9C lea eax, dword ptr [ebp-64]
000113BB . 50 push eax
000113BC . FF15 9CAB010 call dword ptr [<&USER32.RegisterCla
000113C2 . 66:85C0 test ax, ax
000113C5 . 74 75 je short 0001143C
000113C7 . 6A 00 push 0
000113C9 . 56 push esi
000113CA . 6A 00 push 0
000113CC . 6A 00 push 0
000113CE . 6A 78 push 78
000113D0 . 68 F0000000 push 0F0
pWndClassEx
RegisterClassExA
lParam = NULL
hInst
hMenu = NULL
hParent = NULL
Height = 78 (120.)
Width = F0 (240.)
WS_OVERLAPPED|WS_MINIMIZEBOX|WS_MAXIMI
68 0000CF00
8D45 EA lea
50 push
eax, dword ptr [ebp-16]
eax
50 push eax
68 00020000 push 200
FF15 A0AB010 call dword ptr [<&USER32.CreateWindo
CreateWindowExA
WS_EX_CLIENTEDGE
89C6 mov esi, eax
85F6 test esi,esi
short 00011A3C
SW_HIDE
0
esi
call dword ptr [<&USER32.UpdateWindo
jmp


景云杀毒-实时监控
.Trojan-Ransom.WannaCry.Y2.zav
病毒名称：
wannasister.exe
病毒文件：
cuments and Settings\PC\桌面
文件路径：
信任
立即清除


景云杀毒
险类型
风险信息
处理建议
意木马
Win32.Trojan-Ransom.WannaCry.Y2.zav
C:\Documents and Settings\PC\桌面\wannasister.exe
建议删除
病毒查杀
实时防护
常用工具
防护日志
信任与隔离


景云网络防病毒系统
6
super
退出
安全概况
APT 规则
终端监控
信任管理


文件信息
文件名 wannasister
文件类型 exe
4.5 MB
:17:46
扫描时间 2017-05-17 10
MD5
SHA1
SHA256
静态检测
动态检测
件版本： Adobe Reader 11
束时间： 2017-05-17 10:21:32
操作系统： Windows XP SP3
开始时间： 2017-05-17 10:17:59
勒索软件 [1]
notepad.exe的勒索行为报警
PID
进程名
详细信息
moves indicative of a potential file encryption process
996
C:\WINDOWS\system32\notepad.exe
file_modifications: Performs 245 file
new file extension to multiple modified files
996
C:\WINDOWS\system32\notepad.exe
appends_new_extension: Appends a
RY
996
C:\WINDOWS\system32\notepad.exe
new_appended_file_extension: .WNC
RYT
996
C:\WINDOWS\system32\notepad.exe
new_appended_file_extension: .WNC
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
勒索软件程序被写入到notepad.exe中
C:\Documents and Setting
s\Administrator\Local Settin
gs\Temp\wannasister.exe
ProcessName: \Device\HarddiskVolume1\WINDOWS\syste
1092
反虚拟机 [1]
高并发 [1]
反检测 [1]
反调试 [1]
威胁行为 [9]

VenusEye

“ ”

Hedwig