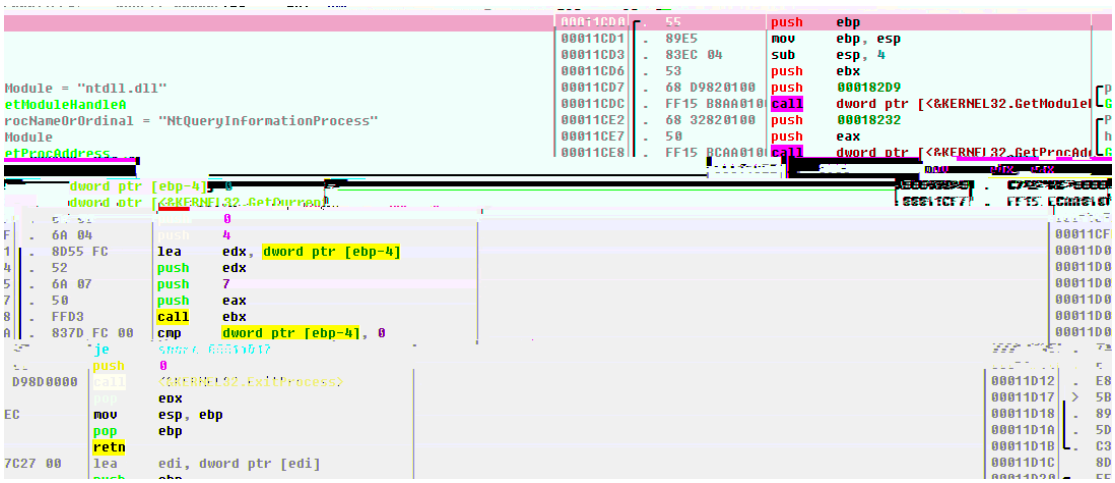
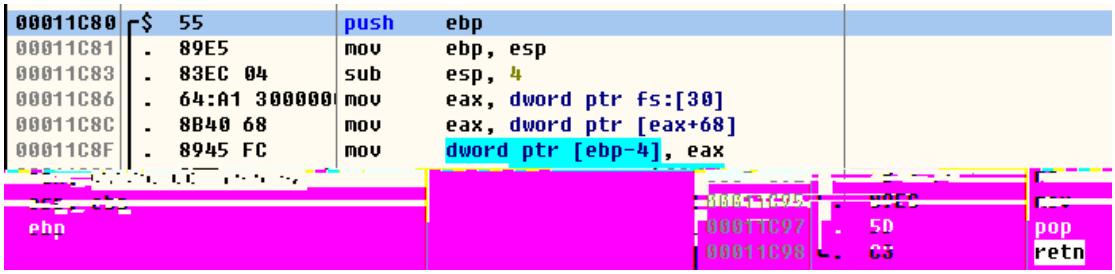
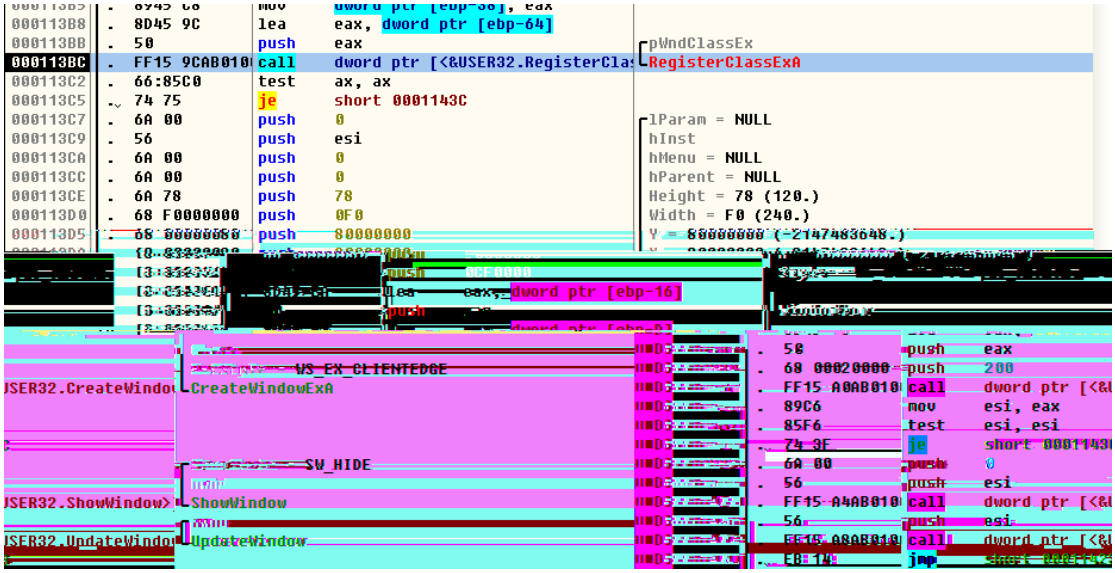
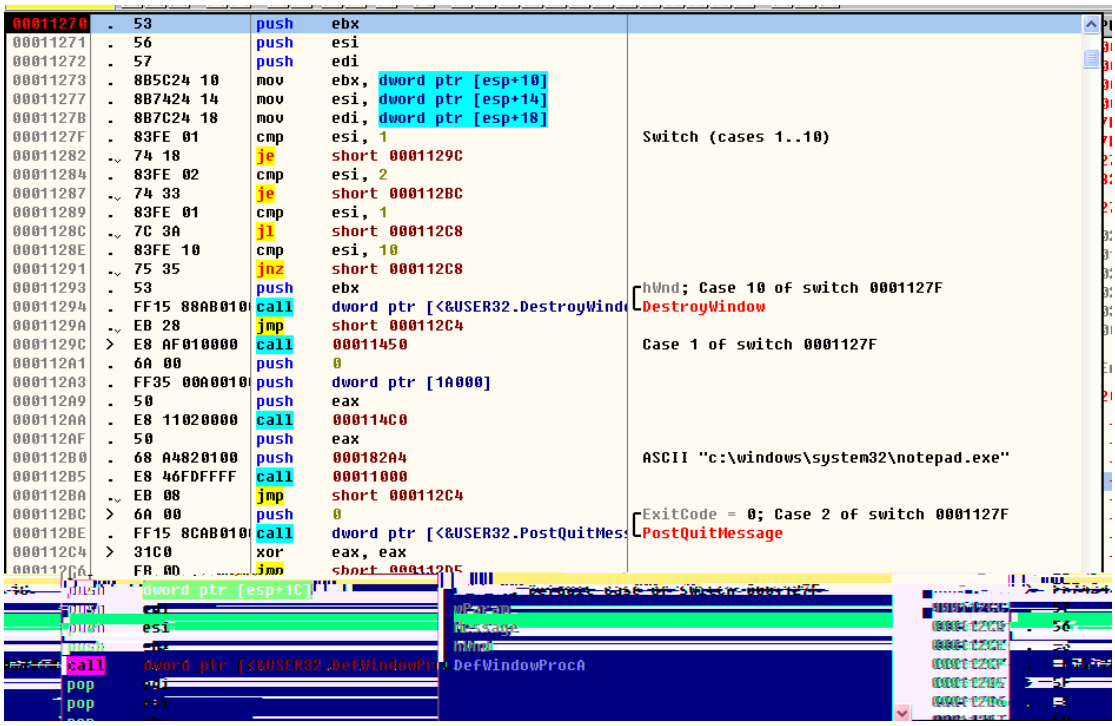
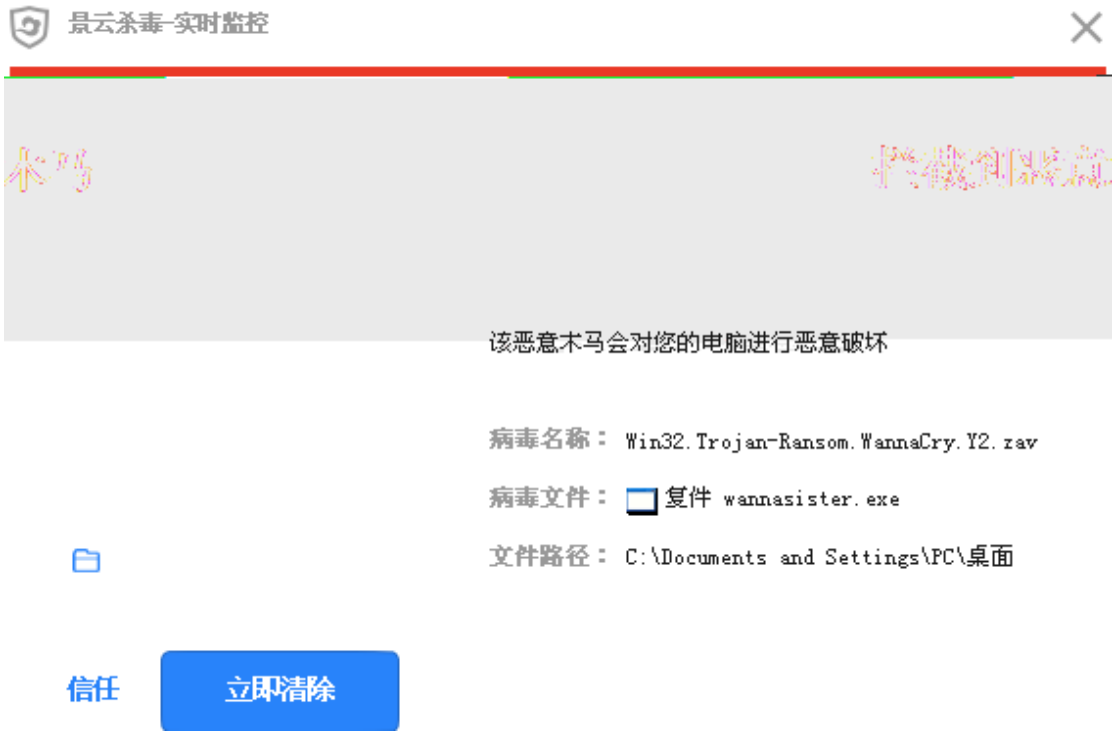

Module = "ntdll.dll"
etModuleHandleA
rocNameOrOrdinal = "NtQueryInformationProcess"
Module
etProcAddress
00011CD1 . 89E5 mov ebp, esp
00011CD3 . 83EC 04 sub esp, 4
00011CD6 . 53 push ebx
00011CD7 . 68 D9820100 push 000182D9
00011CDC . FF15 B8AA0100 call dword ptr [<&KERNEL32.GetModuleH
00011CE2 . 68 32820100 push 00018232
00011CE7 . 50 push eax
00011CE8 . FF15 BCAA0100 call dword ptr [<&KERNEL32.GetProcAdd
dword ptr [ebp-4]
dword ptr [<&KERNEL32.GetCurrentP
0
6A 04 push 4
8D55 FC lea edx, dword ptr [ebp-4]
52 push edx
6A 07 push 7
50 push eax
FFD3 call ebx
837D FC 00 cmp dword ptr [ebp-4], 0
je
push 0
D98D0000 call
edx
EC mov esp, ebp
pop ebp
retn
7C27 00 lea edi, dword ptr [edi]
00011D12 . E8
00011D17 > 5B
00011D18 . 89
00011D1A . 5D
00011D1B . C3
00011D1C 8D

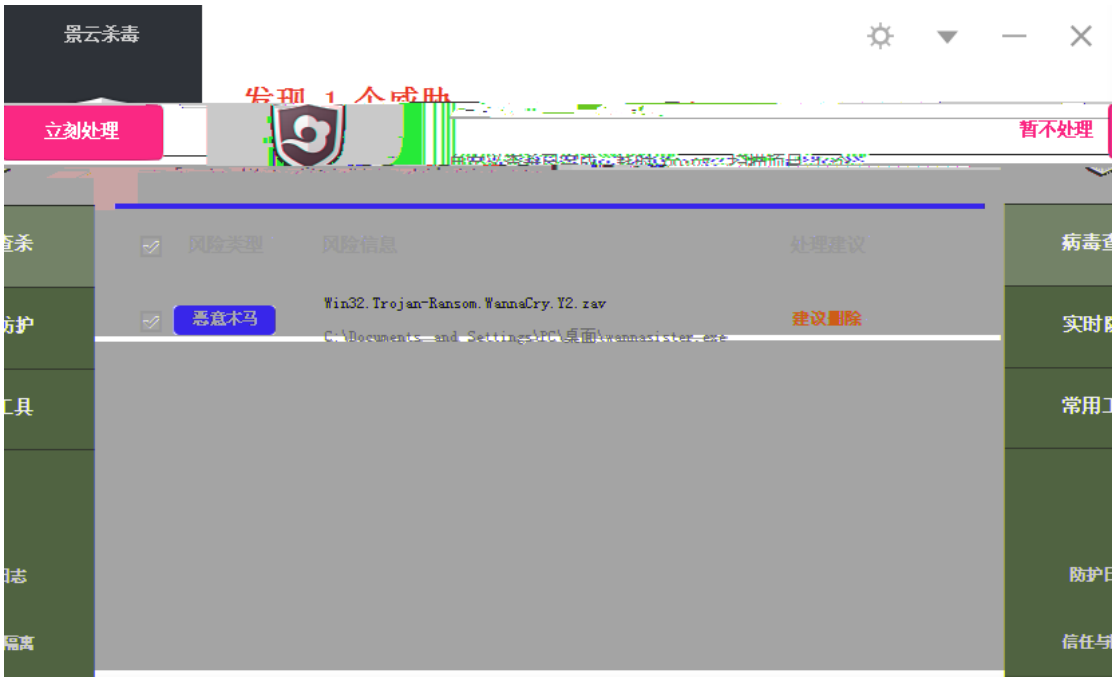

00011C80 $ 55 push ebp
00011C81 . 89E5 mov ebp, esp
00011C83 . 83EC 04 sub esp, 4
00011C86 . 64:A1 300000 mov eax, dword ptr fs:[30]
00011C8C . 8B40 68 mov eax, dword ptr [eax+68]
00011C8F . 8945 FC mov dword ptr [ebp-4], eax
ebp
00011C97 . 5D pop
00011C98 . C3 retn

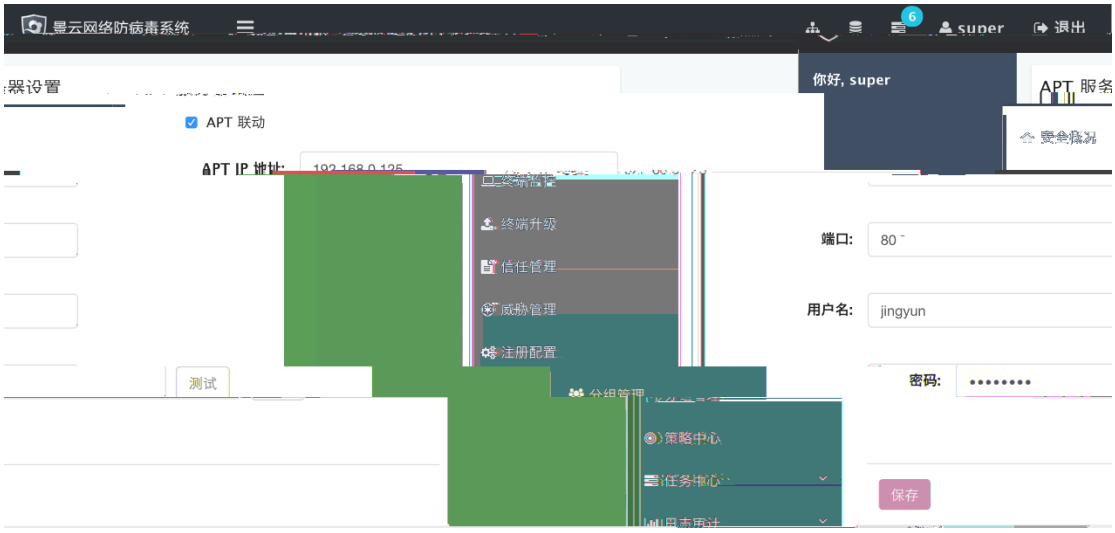
```
00011BAF      00          db      00
00011BB0  $   55          push    ebp
00011BB1  .   89E5        mov     ebp, esp
00011BB3  .   CD 01       int     1
00011BB5  .   B8 55730880 mov     eax, 80087355
00011BBA  .   FFE0        jmp     eax
00011BBC  .   89EC        mov     esp, ebp
00011BBE  .   5D          pop     ebp
00011BBF  .   C3          retn
00011BC0  ┌.  55          push    ebp
```

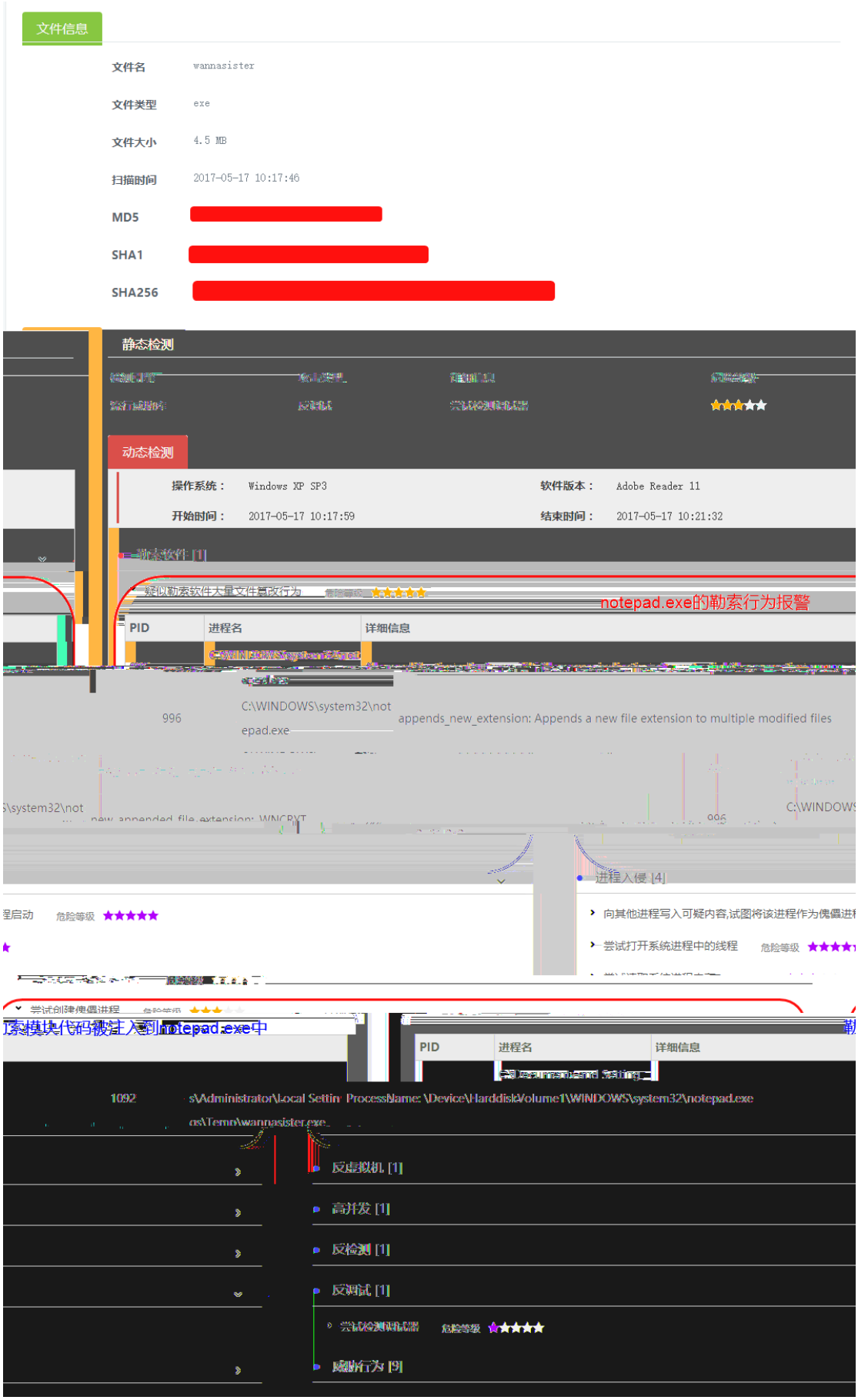





景云杀毒-实时监控
该恶意木马会对您的电脑进行恶意破坏
病毒名称： Win32.Trojan-Ransom.WannaCry.Y2.zav
病毒文件： 复件 wannasister.exe
文件路径： C:\Documents and Settings\PC\桌面
信任
立即清除


景云杀毒
立刻处理
暂不处理
风险类型
风险信息
处理建议
恶意木马
Win32.Trojan-Ransom.WannaCry.Y2.zav
建议删除


昱云网络防病毒系统
super
退出
你好, super
APT 联动
APT IP 地址:
终端升级
信任管理
威胁管理
注册配置
策略中心
任务中心
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
SHA1
SHA256
静态检测
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
notepad.exe的勒索行为报警
PID
进程名
详细信息
996
C:\WINDOWS\system32\notepad.exe
appends_new_extension: Appends a new file extension to multiple modified files
进程入侵 [4]
危险等级
向其他进程写入可疑内容,试图将该进程作为傀儡进程
尝试打开系统进程中的线程
尝试创建傀儡进程
勒索模块代码被注入到notepad.exe中
1092
ProcessName: \Device\HarddiskVolume1\WINDOWS\system32\notepad.exe
C:\Temp\wannasister.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
危险行为 [9]

VenusEye

Hedwig Locky

18 Sage 2.0

Office 0day

2016