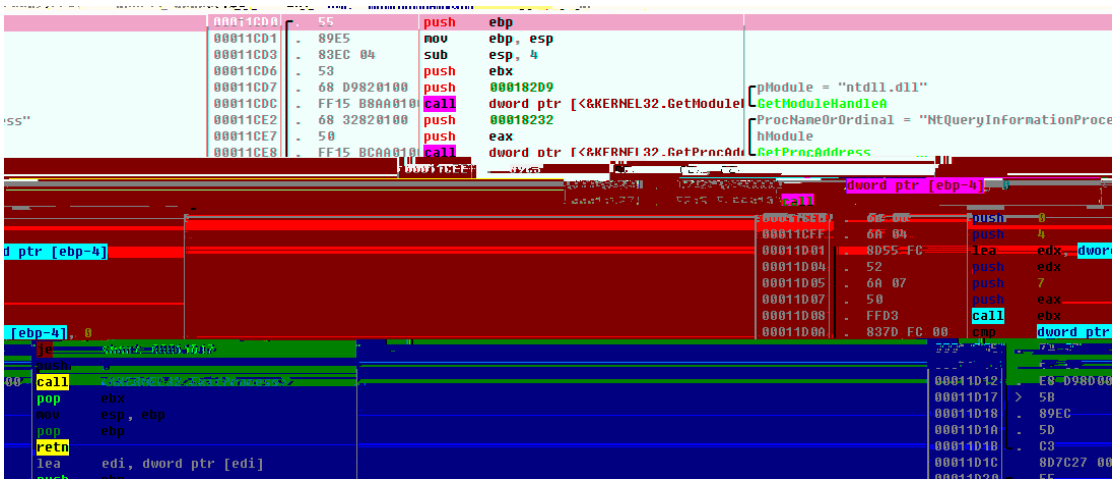
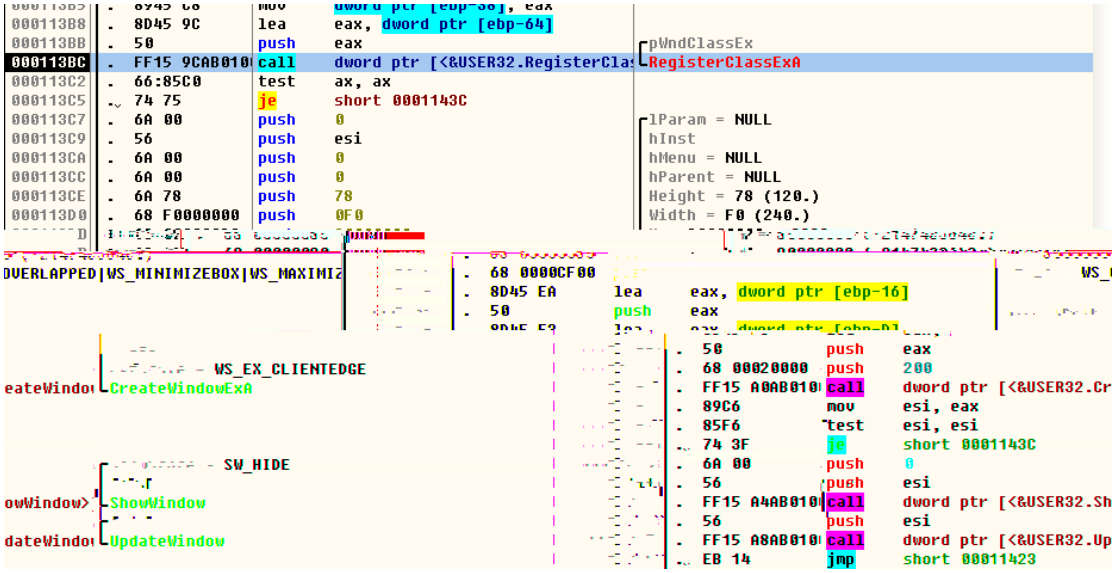
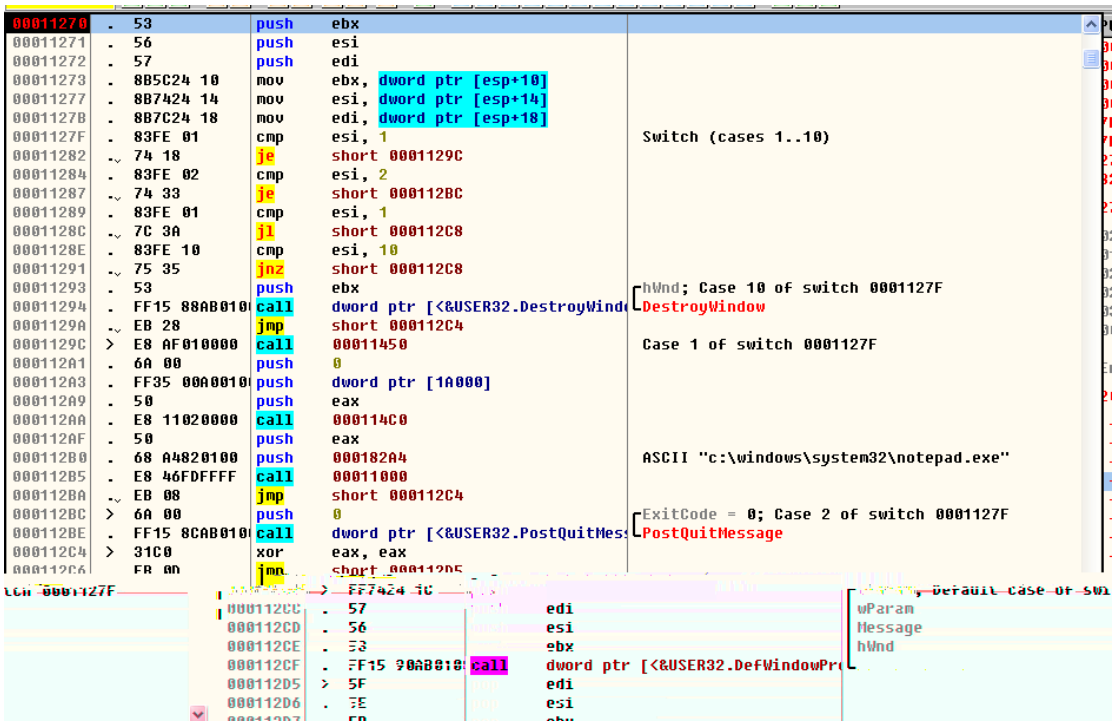
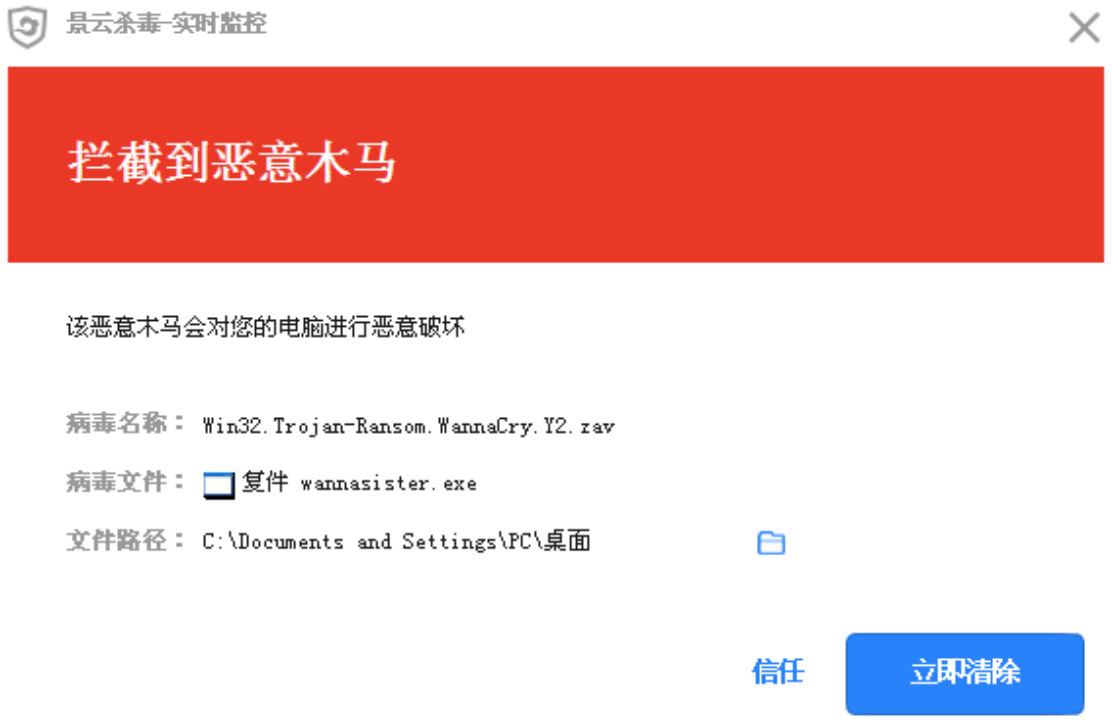



```
00011C80  $  55              push    ebp
00011C81  .  89E5            mov     ebp, esp
00011C83  .  83EC 04         sub     esp, 4
00011C86  .  64:A1 300000    mov     eax, dword ptr fs:[30]
00011C8C  .  8B40 68         mov     eax, dword ptr [eax+68]
00011C8F  .  8945 FC         mov     dword ptr [ebp-4], eax
00011C92  .  8B45 FC         mov     eax, dword ptr [ebp-4]
00011C95  .  89EC            mov     esp, ebp
00011C97  .  5D              pop     ebp
00011C98  L. C3              retn
```

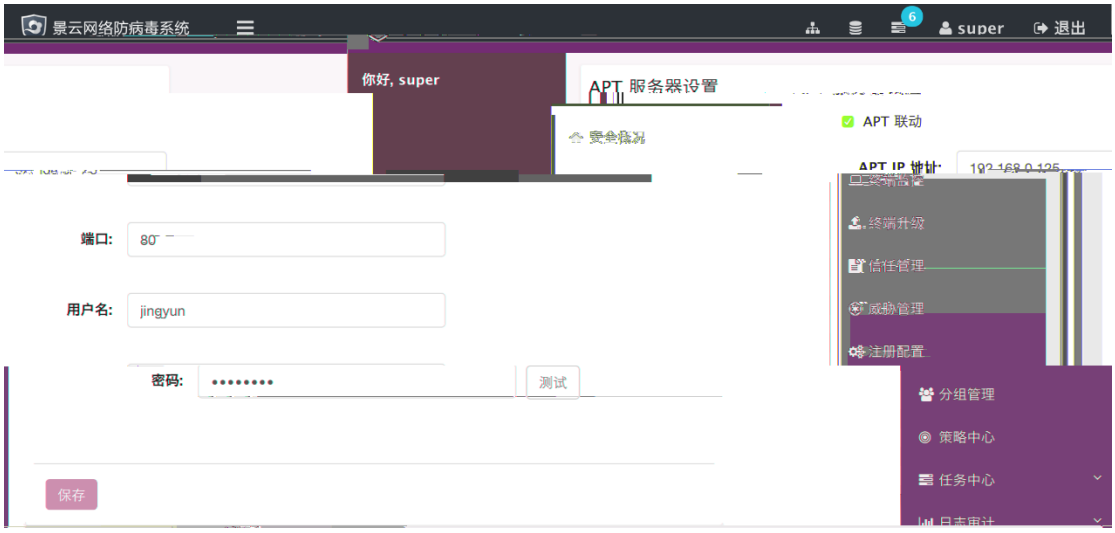
```
00011BAF      00          db      00
00011BB0  $   55          push    ebp
00011BB1  .   89E5        mov     ebp, esp
00011BB3  .   CD 01       int     1
00011BB5  .   B8 55730880 mov     eax, 80087355
00011BBA  .   FFE0        jmp     eax
00011BBC  .   89EC        mov     esp, ebp
00011BBE  .  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





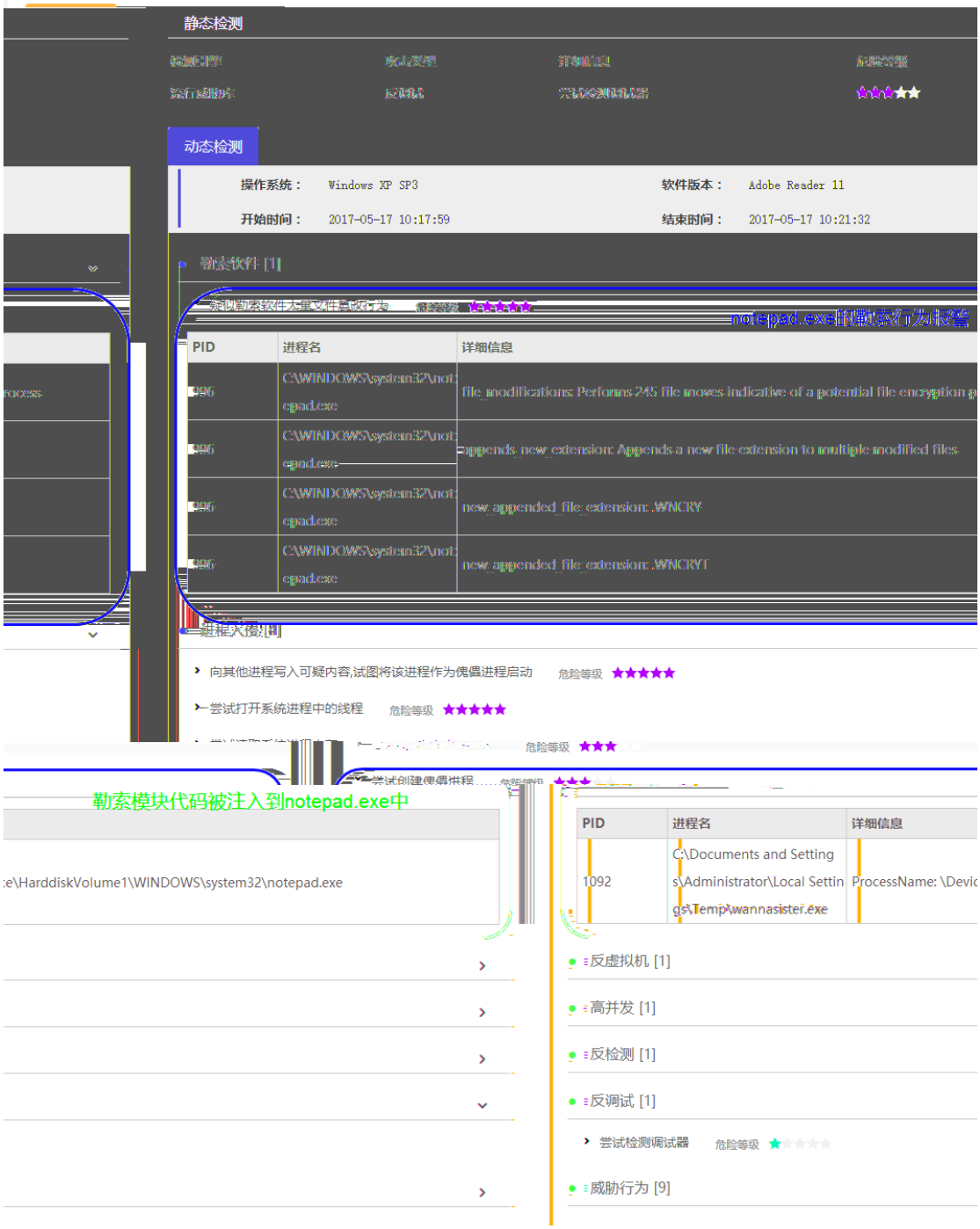

景云杀毒-实时监控
拦截到恶意木马
该恶意木马会对您的电脑进行恶意破坏
病毒名称： Win32.Trojan-Ransom.WannaCry.Y2.zav
病毒文件： 复件 wannasister.exe
文件路径： C:\Documents and Settings\PC\桌面
信任
立即清除


景云杀毒
暂不处理
立刻处理
处理建议
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
风险类型
风险信息
恶意木马


景云网络防病毒系统
6
super
退出
你好, super
APT 服务器设置
APT 联动
端口:
80
用户名:
jingyun
密码:
测试
保存
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

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]



VenusEye

Hedwig Locky

18 Sage 2.0

Office 0day

2016