

“

”

“

”

“

öjō

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

发现 1 个威胁

病毒查杀

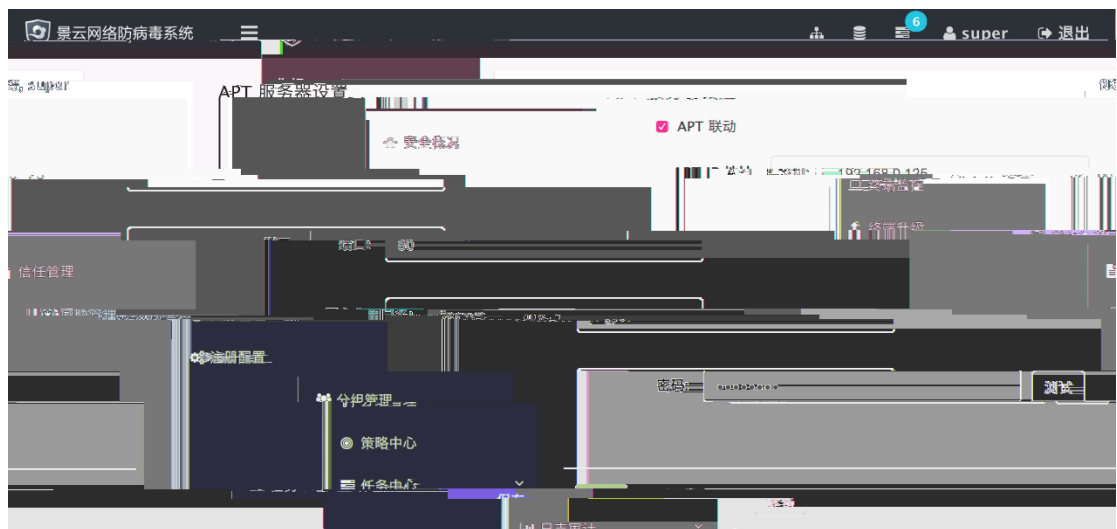
实时防护

常用工具

防护日志

信任与隔离

☒	风险类型	风险信息	处理建议
☒	恶意木马	Win32.Trojan-Ransom.WannaCry.Y2.zav	建议删除



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

尝试检测调试器

流行威胁库

反调试

软件版本：Adobe Reader 11

结束时间：2017-05-17 10:21:32

notepad.exe的勒索行为报警

ications: Performs 245 file moves indicative of a potential file encryption process

new_extension: Appends a new file extension to multiple modified files

ended_file_extension: .WNCRY

ended_file_extension: .WNCRYT

动态检测

操作系统：Windows XP SP3

开始时间：2017-05-17 10:17:59

勒索软件 [1]

疑似勒索软件大量文件篡改行为

危险等级

★★★★★

PID	进程名	详细信息
996	C:\WINDOWS\system32\notepad.exe	file_modif
996	C:\WINDOWS\system32\notepad.exe	appends_i
996	C:\WINDOWS\system32\notepad.exe	new_appe
996	C:\WINDOWS\system32\notepad.exe	new_appe

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

★★★★★

勒索模块代码被注入到notepad.exe

PID	进程名	详细信息
1092	C:\Documents and Settings\Administrator\Local Settings\Temp\wannasister.exe	ProcessName: \Device\HarddiskV...

反虚拟机 [1]

高并发 [1]

反检测 [1]

反调试 [1]

威胁行为 [1]

VenusEye

“ ”

Hedwig

