

“

”

”wannasister”

“

”

“

öjõ

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

病毒名称：Win32.Trojan-Ransom.WannaCry.Y2.zav

文件路径：C:\Documents and Settings\PC\桌面\wannasister.exe

处理建议：建议删除

病毒查杀

实时防护

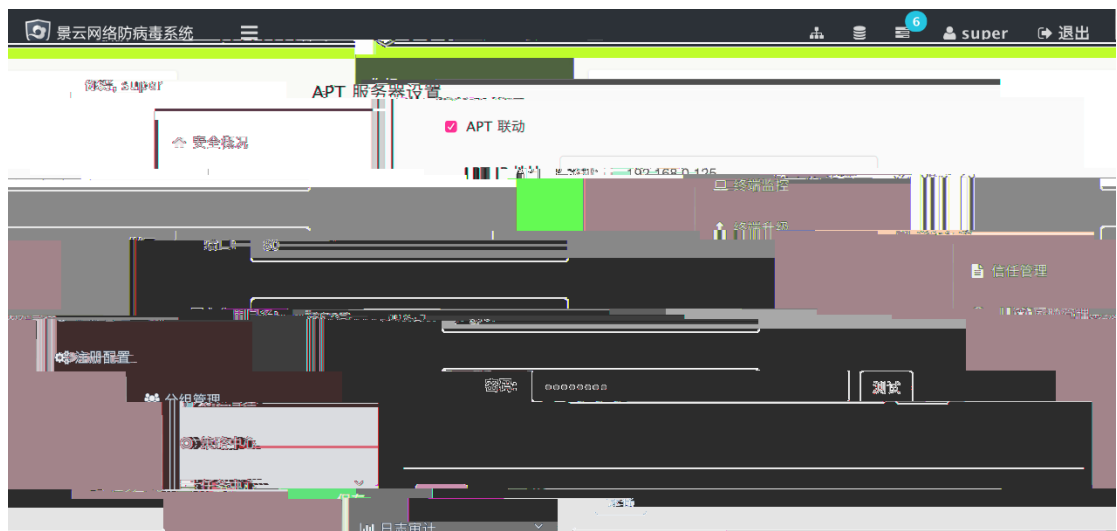
常用工具

防护日志

信任与隔离

风险类型

恶意木马



文件信息

文件名 wannasister
文件类型 exe
文件大小 4.5 MB

:17:46

扫描时间 2017-05-17 10

MD5

SHA1

SHA256

静态检测

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: .WNCRYPT

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 ★★★★★

勒索软件入侵并注入notepad.exe!

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]
威胁行为 [9]

VenusEye

“ ”

Hedwig

