# 永恒之蓝挖矿蠕虫WannaMine特征、行为分析及清除

**背景介绍**

永恒之蓝是指2017年5月13日起，全球范围内爆发的基于Windows网络共享协议进行攻击传播的蠕虫恶意代码，不法分子通过改造之前泄露的NSA黑客武器库中“永恒之蓝”攻击程序发起的网络攻击事件。英国、俄罗斯、整个欧洲以及中国国内多个高校校内网、大型企业内网和政府机构专网中招，被勒索支付高额赎金才能解密恢复文件。

永恒之蓝挖矿蠕虫WannaMine就是利用永恒之蓝漏洞进行传播，与WannaCry勒索病毒不同的是，其不再勒索，而是长期潜伏挖矿，会悄悄的耗尽计算机资源。

**病毒清除方法**

**1. 修复漏洞，杜绝再次感染**

**1.1 执行以下脚本禁用445及部分端口，杜绝被再次感染**

netsh ipsec static delete policy name = SECCPP

netsh ipsec static add policy name = SECCPP description=安全策略201705

netsh ipsec static add filteraction name = Block action = block

netsh ipsec static add filterlist name = SECCPF

netsh ipsec static add filter filterlist = SECCPF srcaddr=Any dstaddr = Me dstport = 135 protocol = TCP

netsh ipsec static add filter filterlist = SECCPF srcaddr=Any dstaddr = Me dstport = 137 protocol = TCP

netsh ipsec static add filter filterlist = SECCPF srcaddr=Any dstaddr = Me dstport = 138 protocol = TCP

netsh ipsec static add filter filterlist = SECCPF srcaddr=Any dstaddr = Me dstport = 139 protocol = TCP

netsh ipsec static add filter filterlist = SECCPF srcaddr=Any dstaddr = Me dstport = 445 protocol = TCP

netsh ipsec static add filter filterlist = SECCPF srcaddr=Any dstaddr = Me dstport = 137 protocol = UDP

netsh ipsec static add filter filterlist = SECCPF srcaddr=Any dstaddr = Me dstport = 138 protocol = UDP

netsh ipsec static add rule name=SECCPR policy=SECCPP filterlist=SECCPF filteraction=Block

netsh ipsec static set policy name = SECCPP assign = y

pause

exit

**1.2 安装微软针对远程代码执行漏洞的补丁**

[MS17-010](https://docs.microsoft.com/zh-cn/security-updates/Securitybulletins/2017/ms17-010)

**2. 永恒之蓝wannacry勒索蠕虫相关进程及文件清除**

执行以下脚本进行清除：

@echo off

>nul 2>&1 "%SYSTEMROOT%\system32\cacls.exe" "%SYSTEMROOT%\system32\config\system"

if '%errorlevel%' NEQ '0' (

goto UACPrompt

) else ( goto gotAdmin )

:UACPrompt

echo Set UAC = CreateObject^("Shell.Application"^) > "%temp%\getadmin.vbs"

echo UAC.ShellExecute "%~s0", "", "", "runas", 1 >> "%temp%\getadmin.vbs"

"%temp%\getadmin.vbs"

exit /B

:gotAdmin

if exist "%temp%\getadmin.vbs" ( del "%temp%\getadmin.vbs" )

cd /d "C:/Windows/"

taskkill /im mssecsvc.exe /f

taskkill /im tasksche.exe /f

del mssecsvc.exe /q

del qeriuwjhrf /q

del tasksche.exe /q

taskkill /im mssecsvc.exe /f

taskkill /im tasksche.exe /f

del mssecsvc.exe /q

del qeriuwjhrf /q

del tasksche.exe /q

**3. 永恒之蓝WannaMine挖矿蠕虫相关进程及文件清除**

执行以下脚本进行清除：

@echo off

>nul 2>&1 "%SYSTEMROOT%\system32\cacls.exe" "%SYSTEMROOT%\system32\config\system"

if '%errorlevel%' NEQ '0' (

goto UACPrompt

) else ( goto gotAdmin )

:UACPrompt

echo Set UAC = CreateObject^("Shell.Application"^) > "%temp%\getadmin.vbs"

echo UAC.ShellExecute "%~s0", "", "", "runas", 1 >> "%temp%\getadmin.vbs"

"%temp%\getadmin.vbs"

exit /B

:gotAdmin

if exist "%temp%\getadmin.vbs" ( del "%temp%\getadmin.vbs" )

sc stop wmassrv

sc delete wmassrv

taskkill /IM spoolsv.exe /f

taskkill /IM rundll32.exe /f

wmic process get ProcessId,executablepath | findstr "C:\Windows\SpeechsTracing" > 1.txt

for /f "delims=" %%i in ("1.txt") do (for /f "tokens=2" %%m in (%%i) do (taskkill /PID %%m /f))

del 1.txt

del C:\Windows\system32\wmassrv.dll

del C:\Windows\system32\HalPluginsServices.dll

del C:\Windows\System32\EnrollCertXaml.dll

del C:\Windows\SpeechsTracing\spoolsv.exe

del C:\Windows\SpeechsTracing\Microsoft\\*.exe

rd /s /q C:\Windows\SpeechsTracing

**永恒之蓝挖矿蠕虫WannaMine特征、行为分析**

该文章对蠕虫原理进行了专业描述，可论证上述结论的正确性：[WMAMiner挖矿蠕虫分析](https://www.sohu.com/a/233033942_354899)

**永恒之蓝挖矿蠕虫WannaMine特征**

**特征1：出现以下文件及目录**

C:\Windows\system32\HalPluginsServices.dll

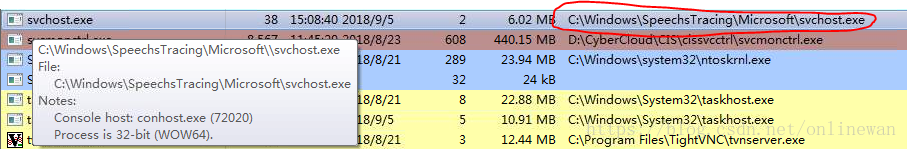
C:\Windows\System32\EnrollCertXaml.dll

C:\Windows\SpeechsTracing

C:\Windows\SpeechsTracing\Microsoft\

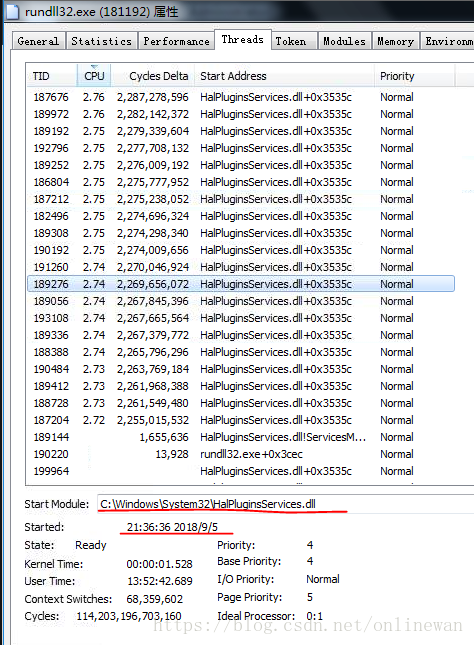
**特征2：出现两个spoolsv.exe进程**

出现一个非system32目录的svchost.exe进程



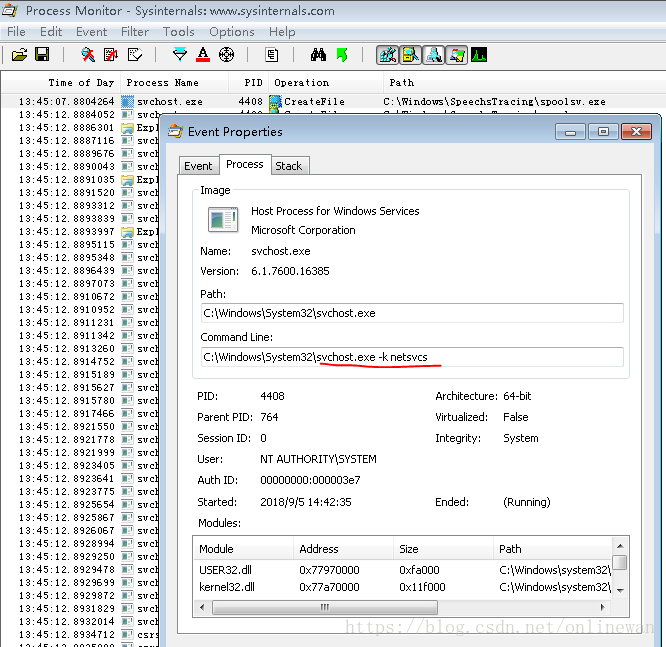
**特征3：打开任务管理器时CPU占用下降，关闭后cpu占用又升高，升高时会有一个rundll32.exe进程启动**

如下：

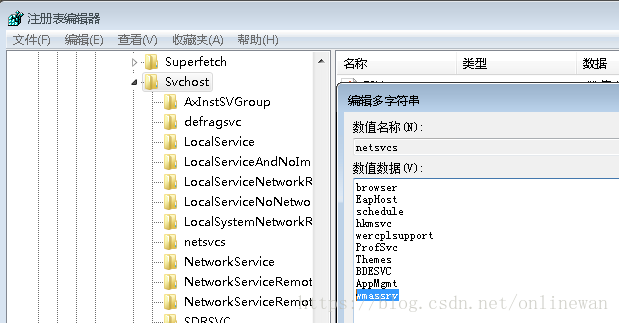


**蠕虫行为分析及清除脚本**

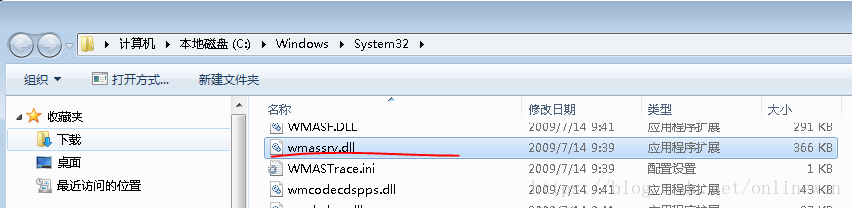
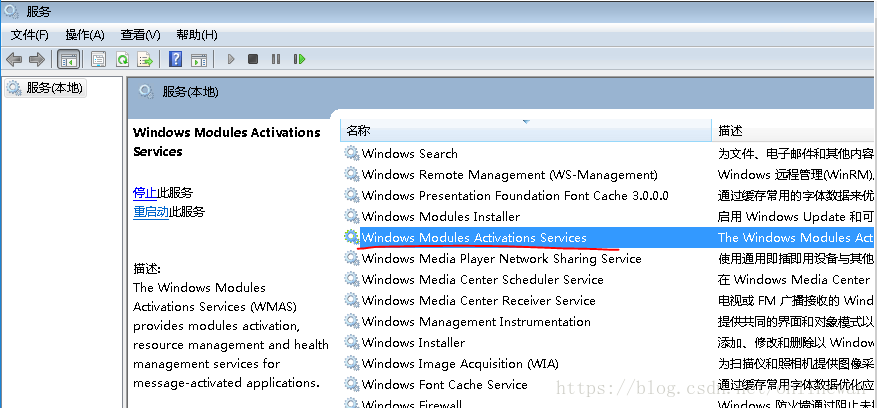
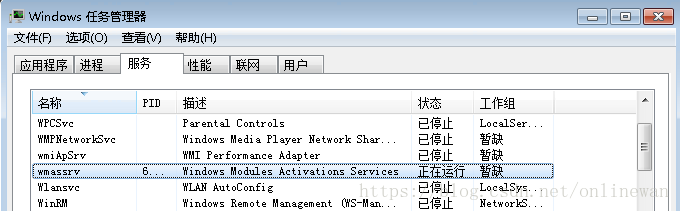
**步骤1：使用ProcessMon查看spoolsv、rundll32进程都是被以下进程启动**



**步骤2：查看 netsvcs 配置的自启动服务列表发现有一个新增的wmassrv**



**步骤3：查看该服务信息**



**步骤4：到此猜测如果把该服务关了是否spoolsv.exe等进程就不会再被创建，进行尝试**

发现关了该服务后，手动杀掉spoolsv.exe rundll32.exe进程都不会再自动启动。至此回忆该服务为其伪装的守护服务。

**步骤5：编写脚本停服务、删除服务、杀进程，及相关文件(务必以管理员权限)**

@echo off

>nul 2>&1 "%SYSTEMROOT%\system32\cacls.exe" "%SYSTEMROOT%\system32\config\system"

if '%errorlevel%' NEQ '0' (

goto UACPrompt

) else ( goto gotAdmin )

:UACPrompt

echo Set UAC = CreateObject^("Shell.Application"^) > "%temp%\getadmin.vbs"

echo UAC.ShellExecute "%~s0", "", "", "runas", 1 >> "%temp%\getadmin.vbs"

"%temp%\getadmin.vbs"

exit /B

:gotAdmin

if exist "%temp%\getadmin.vbs" ( del "%temp%\getadmin.vbs" )

sc stop wmassrv

sc delete wmassrv

taskkill /IM spoolsv.exe /f

taskkill /IM rundll32.exe /f

wmic process get ProcessId,executablepath | findstr "C:\Windows\SpeechsTracing" > 1.txt

for /f "delims=" %%i in ("1.txt") do (for /f "tokens=2" %%m in (%%i) do (taskkill /PID %%m /f))

del 1.txt

del C:\Windows\system32\wmassrv.dll

del C:\Windows\system32\HalPluginsServices.dll

del C:\Windows\System32\EnrollCertXaml.dll

del C:\Windows\SpeechsTracing\spoolsv.exe

del C:\Windows\SpeechsTracing\Microsoft\\*.exe

rd /s /q C:\Windows\SpeechsTracing

**步骤6：重启机器检测，再未发现异常症状**

确认采用上述脚本可彻底清除挖矿蠕虫。

上述脚本可用于快速清除挖矿蠕虫，为了安全起见，还是应该及时打系统补丁并安装杀毒软件。