

第6篇：挖矿病毒（二）

0x00 前言

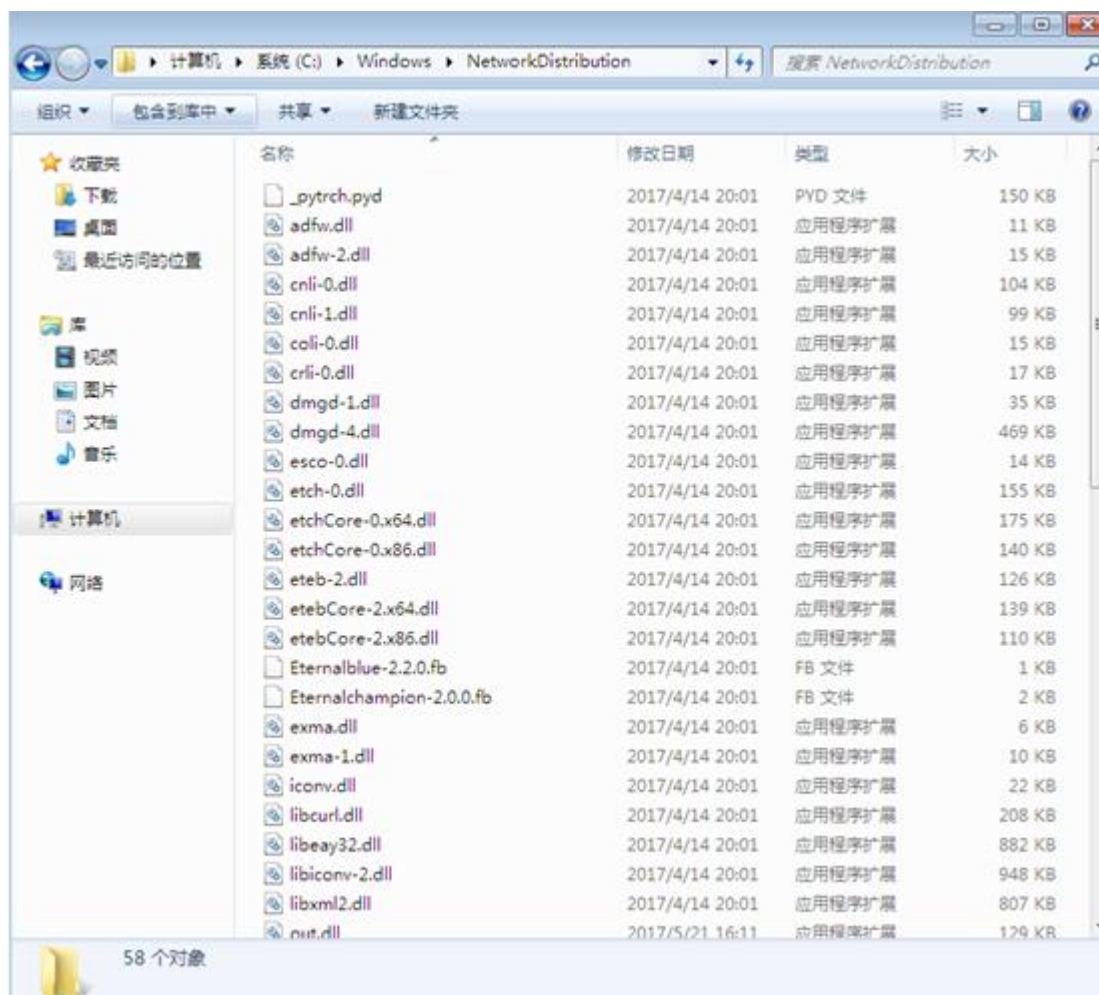
作为一个运维工程师，而非一个专业的病毒分析工程师，遇到了比较复杂的病毒怎么办？别怕，虽然对二进制不熟，但是依靠系统运维的经验，我们可以用自己的方式来解决它。

0x01 感染现象

1、向大量远程IP的445端口发送请求

```
C:\Users\Administrator>netstat -ano | find "SYN"
TCP 169.254.1.2:173:61297 169.254.1.2:173:445 SYN_SENT 32740
TCP 169.254.1.2:173:61298 169.254.1.2:173:445 SYN_SENT 32740
TCP 169.254.1.2:173:61299 169.254.1.2:173:445 SYN_SENT 32740
TCP 169.254.1.2:173:61300 169.254.1.2:173:445 SYN_SENT 32740
TCP 169.254.1.2:173:61301 169.254.1.2:173:445 SYN_SENT 32740
TCP 169.254.1.2:173:61302 169.254.1.2:173:445 SYN_SENT 32740
TCP 169.254.1.2:173:61303 169.254.1.2:173:445 SYN_SENT 32740
TCP 169.254.1.2:173:61304 169.254.1.2:173:445 SYN_SENT 32740
TCP 169.254.1.2:173:61305 169.254.1.2:173:445 SYN_SENT 32740
TCP 169.254.1.2:173:61306 169.254.1.2:173:445 SYN_SENT 32740
TCP 169.254.1.2:173:61307 169.254.1.2:173:445 SYN_SENT 32740
TCP 169.254.1.2:173:61308 169.254.1.2:173:445 SYN_SENT 32740
TCP 169.254.1.2:173:61309 169.254.1.2:173:445 SYN_SENT 32740
TCP 169.254.1.2:173:61310 169.254.1.2:173:445 SYN_SENT 32740
TCP 169.254.1.2:173:61311 169.254.1.2:173:445 SYN_SENT 32740
TCP 169.254.1.2:173:61312 169.254.1.2:173:445 SYN_SENT 32740
TCP 169.254.1.2:173:61313 169.254.1.2:173:445 SYN_SENT 32740
TCP 169.254.1.2:173:61314 169.254.1.2:173:445 SYN_SENT 32740
TCP 169.254.1.2:173:61315 169.254.1.2:173:445 SYN_SENT 32740
TCP 169.254.1.2:173:61316 169.254.1.2:173:445 SYN_SENT 32740
TCP 169.254.1.2:173:61317 169.254.1.2:173:445 SYN_SENT 32740
```

2、使用各种杀毒软件查杀无果，虽然能识别出在C:\Windows\NetworkDistribution中发现异常文件，但即使删除NetworkDistribution后，每次重启又会再次生成。



连杀软清除不了的病毒，只能手工来吧，个人比较偏好火绒，界面比较简洁，功能也挺好用的，自带的火绒剑是安全分析利器。于是安装了火绒，有了如下分析排查过程。

0x02 事件分析

A、网络链接

通过现象，找到对外发送请求的进程ID：4960

| 进程名 | 进程ID | 安全状态 | 模块 | 协议 | 本地地址 | 远程地址 | 状态 |
|------------|------|------|--------------------------------|-----|----------------------|-------------------|--------------|
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55954 | 10.101.30.148:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55955 | 10.101.30.148:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55956 | 10.101.30.150:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55957 | 10.101.30.151:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55958 | 10.101.30.152:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55959 | 10.101.30.153:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55960 | 10.101.30.154:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55961 | 10.101.30.155:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55962 | 10.101.30.156:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55963 | 10.101.30.157:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55964 | 10.101.30.158:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55965 | 10.101.30.159:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55966 | 10.101.30.160:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55967 | 10.101.30.161:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55968 | 10.101.30.162:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55969 | 10.101.30.163:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55970 | 10.101.30.164:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55971 | 10.101.30.165:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55972 | 10.101.30.166:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55973 | 10.101.30.167:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55974 | 10.101.30.168:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55975 | 10.101.30.169:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55976 | 10.101.30.170:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55977 | 10.101.30.171:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55978 | 10.101.30.172:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55979 | 10.101.30.173:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55980 | 10.101.30.174:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55981 | 10.101.30.175:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55982 | 10.101.30.176:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55986 | 10.101.30.177:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55994 | 10.101.30.178:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55995 | 10.101.30.179:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:55997 | 10.101.30.180:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:56000 | 10.101.30.181:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:56009 | 10.101.30.182:445 | TS_sync_sent |
| ctfmon.exe | 4960 | 系统文件 | C:\Windows\System32\ctfmon.exe | TCP | 192.168.130.39:56040 | 10.101.30.183:445 | TS_sync_sent |

B、进程分析

进一步通过进程ID找到相关联的进程，父进程为1464

| 进程名 | 进程ID | 任务组ID | 公司名 | 描述 | 路径 |
|-------------------------|-------|-------|-------------------------|--|--|
| wininit.exe | 748 | 0 | Microsoft Corporation | Windows 启动应用程序 | C:\Windows\system32\wininit.exe |
| services.exe | 844 | 0 | Microsoft Corporation | 服务和控制管理器进程 | C:\Windows\system32\services.exe |
| svchost.exe | 968 | 0 | Microsoft Corporation | Windows 服务主进程 | C:\Windows\system32\svchost.exe |
| wmiprvse.exe | 5736 | 0 | Microsoft Corporation | WMI Provider Host | C:\Windows\system32\wbem\wmiprvse.exe |
| unsecapp.exe | 2180 | 0 | Microsoft Corporation | Sink to receive asynchronous callbacks for WMI ... | C:\Windows\system32\wbem\unsecapp.exe |
| wmiprvse.exe | 6628 | 0 | Microsoft Corporation | WMI Provider Host | C:\Windows\system32\wbem\wmiprvse.exe |
| HpsDaemon.exe | 1028 | 0 | 北京火绒网络科技有限公司 | 火绒安全软件 | C:\Program Files\Huorong\HpsDaemon.exe |
| usysdiag.exe | 1128 | 0 | Beijing Huorong Netw... | Huorong Sysdiag Helper | C:\Program Files\Huorong\Sysdiag\bin\usysdiag.exe |
| NVDisplay.Container.exe | 1052 | 1052 | NVIDIA Corporation | NVIDIA Container | C:\Program Files\NVIDIA Corporation\Display\NvContainer\NVDispla |
| NVDisplay.Container.exe | 1756 | 1052 | NVIDIA Corporation | NVIDIA Container | C:\Program Files\NVIDIA Corporation\Display\NvContainer\NVDispla |
| svchost.exe | 1260 | 0 | Microsoft Corporation | Windows 服务主进程 | C:\Windows\system32\svchost.exe |
| svchost.exe | 1368 | 0 | Microsoft Corporation | Windows 服务主进程 | C:\Windows\system32\svchost.exe |
| AUDIODG.EXE | 20856 | 0 | Microsoft Corporation | Windows 音频设备驱动程序 | C:\Windows\system32\AUDIODG.EXE |
| svchost.exe | 1436 | 0 | Microsoft Corporation | Windows 服务主进程 | C:\Windows\system32\svchost.exe |
| WUDFHost.exe | 1924 | 0 | Microsoft Corporation | Windows 驱动程序基础 - 用户模式驱动程序框架主... | C:\Windows\system32\WUDFHost.exe |
| Dum.exe | 3200 | 0 | Microsoft Corporation | 设备驱动程序管理器 | C:\Windows\system32\Dum.exe |
| WSPPTTS.EXE | 19588 | 0 | Microsoft Corporation | Microsoft 手写笔和触控输入组件 | C:\Windows\SYSTEM32\WSPPTTS.EXE |
| svchost.exe | 1464 | 0 | Microsoft Corporation | Windows 服务主进程 | C:\Windows\system32\svchost.exe |
| dllhost.exe | 4540 | 4540 | Microsoft Corporation | COM Surrogate | C:\Windows\system32\dllhost.exe |
| ctfmon.exe | 4960 | 0 | Microsoft Corporation | CTF 加载程序 | C:\Windows\system32\ctfmon.exe |
| taskeng.exe | 12984 | 0 | Microsoft Corporation | 任务计划程序引擎 | C:\Windows\system32\taskeng.exe |
| svchost.exe | 1636 | 0 | Microsoft Corporation | Windows 服务主进程 | C:\Windows\system32\svchost.exe |
| LDsecSvc.EXE | 1740 | 1740 | LANDESK Software, Inc. | LANDESK Endpoint Security | C:\Program Files\LANDESK\LDClient\Hps\LDsecSvc.EXE |
| svchost.exe | 288 | 0 | Microsoft Corporation | Windows 服务主进程 | C:\Windows\system32\svchost.exe |
| spoolsv.exe | 544 | 0 | Microsoft Corporation | 后台处理程序子系统应用程序 | C:\Windows\System32\spoolsv.exe |
| svchost.exe | 476 | 0 | Microsoft Corporation | Windows 服务主进程 | C:\Windows\system32\svchost.exe |
| armvsc.exe | 1524 | 1524 | Adobe Systems Incorp... | Adobe Acrobat Update Service | C:\Program Files\Common Files\Adobe\ARM\1.0\armvsc.exe |
| residentagent.exe | 1768 | 1768 | Ivanti | Resident Agent Application | C:\Program Files\LANDESK\Shared Files\residentagent.exe |
| collector.exe | 2404 | 1768 | LANDESK Software, Inc. | collector Application | C:\Program Files\LANDESK\LDClient\collector.exe |
| svchost.exe | 484 | 0 | Microsoft Corporation | Windows 服务主进程 | C:\Windows\System32\svchost.exe |
| svchost.exe | 2052 | 0 | Microsoft Corporation | Windows 服务主进程 | C:\Windows\System32\svchost.exe |
| IsaHelp.exe | 2108 | 2108 | IsaHelp | 应用程序 | C:\windows\system32\IsaHelp\IsaHelp.exe |
| IsaTel.exe | 3464 | 3464 | IsaTel | 应用程序 | C:\windows\system32\IsaTel\IsaTel.exe |

| 名称 | 安全状态 | 地址 | 大小 | 路径 | 公司名 | 描述 |
|----------------|------|------------|------------|------------------------------------|-----------------------|---------------------------|
| ctfmon.exe | 系统文件 | 0x00060000 | 0x00030000 | C:\Windows\system32\ctfmon.exe | Microsoft Corporation | CTF 加载程序 |
| ntdll.dll | 系统文件 | 0x77940000 | 0x0013C000 | C:\Windows\SYSTEM32\ntdll.dll | Microsoft Corporation | NT 系统 DLL |
| kernel32.dll | 系统文件 | 0x75810000 | 0x000D4000 | C:\Windows\system32\kernel32.dll | Microsoft Corporation | Windows NT 基本 API 客户端 DLL |
| KERNELBASE.dll | 系统文件 | 0x752A0000 | 0x0004A000 | C:\Windows\system32\KERNELBASE.dll | Microsoft Corporation | Windows NT 基本 API 客户端 DLL |

找到进程ID为1464的服务项，逐一排查，我们发现服务项RemoteUPnPService存在异常。

| 名称 | 显示名称 | 安全状态 | 进程ID | 路径 | 描述 | 启动类型 | 状态 |
|-----------------------|-------------------------------------|--------|------|---|---|------|------|
| WlanSvc | WLAN AutoConfig | 系统文件 | 1436 | C:\Windows\System32\wlanautocfg.dll | WLAN AutoConfig 服务提供配置、发现、连接、断开与 IEEE 802.11 无线网络。该服务使用 SSDP/WiFi 协议。 | 手动 | 正在运行 |
| WdiSystemHost | Diagnostic System Host | 系统文件 | 1436 | C:\Windows\System32\wdi.sys | 诊断系统主机被诊断系统服务用来收集数据在本地。 | 手动 | 正在运行 |
| UsSvc | Desktop Window Manager Service | 系统文件 | 1436 | C:\Windows\System32\usm.dll | 提供桌面窗口管理器和维护服务。 | 手动 | 正在运行 |
| TrkWks | Distributed Link Tracking Client | 系统文件 | 1436 | C:\Windows\System32\trkwks.dll | 维护某个计算机内或网络中的计算机的 NTFS 文件。 | 手动 | 正在运行 |
| SysMain | Superfetch | 系统文件 | 1436 | C:\Windows\System32\sysmain.dll | 维护和提高一般时间内的系统性能。 | 手动 | 正在运行 |
| Netman | Network Connections | 系统文件 | 1436 | C:\Windows\System32\netman.dll | 管理“网络和设备连接”文件夹中的对象，在其中也可... | 手动 | 正在运行 |
| CscService | Offline Files | 系统文件 | 1436 | C:\Windows\System32\cscvcs.dll | 脱机文件服务在脱机文件缓存中执行维护活动，例如... | 手动 | 正在运行 |
| AudioEndpointBuilder | Windows Audio Endpoint Builder | 系统文件 | 1436 | C:\Windows\System32\audioendpointbuilder.dll | 管理 Windows 音频服务的音频设备，如果此服务被... | 手动 | 正在运行 |
| wuaueng | Windows Update | 系统文件 | 1464 | C:\Windows\System32\wuaueng.dll | 应用检测、下载和安装 Windows 更新程序更新。 | 手动 | 正在运行 |
| Winmgmt | Windows Management Instrumentation | 系统文件 | 1464 | C:\Windows\System32\wbem\WMI | 提供共同的界面和对象模型以访问有关系统信息... | 手动 | 正在运行 |
| Themes | Themes | 系统文件 | 1464 | C:\Windows\System32\themeservice.dll | 为用户提供使用主题管理的体验。 | 手动 | 正在运行 |
| ShellHWDetection | Shell Hardware Detection | 系统文件 | 1464 | C:\Windows\System32\shhwdet.dll | 为自动播放硬件事件提供通知。 | 手动 | 正在运行 |
| SENS | System Event Notification Service | 系统文件 | 1464 | C:\Windows\System32\sens.dll | 监视系统事件并通知订户这些事件的 COM+ 事件系... | 手动 | 正在运行 |
| Schedule | Task Scheduler | 系统文件 | 1464 | C:\Windows\System32\schedvcs.dll | 使用户可以在此计算机上配置和计划自动任务。此服... | 手动 | 正在运行 |
| RemoteUPnPService | Remote UPnP Service | 未知文件 | 1464 | C:\Windows\System32\RemoteUPnPService.dll | Enables a common interface and object model for... | 手动 | 正在运行 |
| ProfSvc | User Profile Service | 系统文件 | 1464 | C:\Windows\System32\profsvc.dll | 此服务负责加载和卸载用户配置文件。如果已停止或... | 手动 | 正在运行 |
| MMCSS | Multimedia Class Scheduler | 系统文件 | 1464 | C:\Windows\System32\mmcss.dll | 基于系统范围内的任务优先级使用工作的相对优先级... | 手动 | 正在运行 |
| LanmanServer | Server | 系统文件 | 1464 | C:\Windows\System32\lanman.sys | 支持此计算机通过网络的文件、打印、和命名空间。 | 手动 | 正在运行 |
| iphlpvc | IP Helper | 系统文件 | 1464 | C:\Windows\System32\iphlpvc.dll | 使用 IPv6 网络接口 (NIC)、ISATAP、隧道代理和 Ter... | 手动 | 正在运行 |
| DXEEXT | DXE and AuthIP IPsec Keying M... | 系统文件 | 1464 | C:\Windows\System32\dxext.dll | DXEEXT 服务托管 Internet 密钥交换 (IKE) 和身份验证... | 手动 | 正在运行 |
| gpvc | Group Policy Client | 系统文件 | 1464 | C:\Windows\System32\gpvc.dll | 该服务负责通过组策略客户端管理为计算机应用。 | 手动 | 正在运行 |
| EapHost | Extensible Authentication Protoc... | 系统文件 | 1464 | C:\Windows\System32\eaphost.dll | 可扩展的身份验证协议 (EAP) 服务在以下情况下提供网... | 手动 | 正在运行 |
| Browser | Computer Browser | 系统文件 | 1464 | C:\Windows\System32\browser.dll | 维护网络上计算机的更新列表，并将列表提供给计算... | 手动 | 正在运行 |
| BTSS | Background Intelligent Transfer... | 系统文件 | 1464 | C:\Windows\System32\btss.dll | 使用空闲网络带宽在后台传输文件。如果该服务被禁... | 手动 | 正在运行 |
| AsLockupSvc | Application Experience | 系统文件 | 1464 | C:\Windows\System32\aslockupvc.dll | 在应用程序启动时为应用程序处理应用程序性能。 | 手动 | 正在运行 |
| AdobeARMService | Adobe Acrobat Update Service | 数字签名文件 | 1524 | C:\Program Files\Common Files\Adobe\ARM\1.0\AdobeARMService.exe | Adobe Acrobat Updater keeps your Adobe soft... | 手动 | 正在运行 |
| WinHttpAutoProxy | WinHTTP Web Proxy Auto-Disco... | 系统文件 | 1636 | C:\Windows\System32\winhttp.dll | WinHTTP 实现了客户端 HTTP 堆栈并向开发人员提供... | 手动 | 正在运行 |
| WdiServiceHost | Diagnostic System Host | 系统文件 | 1636 | C:\Windows\System32\wdi.sys | 诊断系统主机被诊断系统服务用来收集数据在本地。 | 手动 | 正在运行 |
| W32Time | Windows Time | 系统文件 | 1636 | C:\Windows\System32\w32time.dll | 维护在网络上所有客户端和服务器的时间和日期。 | 手动 | 正在运行 |
| nsi | Network Store Interface Service | 系统文件 | 1636 | C:\Windows\System32\nsi.sys | 此服务向用户模式客户端提供网络地址和协议。添加... | 手动 | 正在运行 |
| netprofm | Network List Service | 系统文件 | 1636 | C:\Windows\System32\netprofm.dll | 识别计算机已连接的网络，收集和存储这些网络的属... | 手动 | 正在运行 |
| EventSystem | COM+ Event System | 系统文件 | 1636 | C:\Windows\System32\es.dll | 支持系统事件通知 (SENS)，此服务为订阅的组件。 | 手动 | 正在运行 |
| LDSEvc | LANDESK Endpoint Security | 数字签名文件 | 1740 | C:\Program Files\LANDESK\LDClient\Nps\LDSEvc.exe | 提供对工作站的主动防御：HIPS、白名单、防火墙、设... | 手动 | 正在运行 |
| CBAS | LANDESK(R) Management Agent | 未知文件 | 1768 | C:\Program Files\LANDESK\Shared Files\resid... | Provides management services for LANDESK(R) p... | 手动 | 正在运行 |
| QPCore | QPCore Service | 数字签名文件 | 1908 | C:\Program Files\Common Files\Tencent\QQP... | 腾讯安全服务 | 手动 | 正在运行 |
| FastUserSwitching... | FastUserSwitchingCompatibility | 数字签名文件 | 2052 | C:\Windows\System32\lsagent\lsagent.exe | 快速用户切换兼容性 | 手动 | 正在运行 |
| Intel Local Schedu... | Intel Local Scheduler Service | 数字签名文件 | 2136 | C:\Program Files\Intel\Intel(R) Management... | 英特尔本地调度器服务 | 手动 | 正在运行 |
| Intel PDS | Intel PDS | 未知文件 | 2304 | C:\Windows\System32\CBAS\pds.exe | 英特尔平台驱动程序 | 手动 | 正在运行 |
| ISSUSER | LANDESK 进程支持服务 | 数字签名文件 | 2428 | C:\Program Files\LANDESK\LDClient\issuser.exe | 允许来自内部服务器部门或 IT 部门的进程支持。 | 手动 | 正在运行 |
| LANDESK Targeted... | LANDESK 定向多播 | 数字签名文件 | 2600 | C:\Program Files\LANDESK\LDClient\lmcscv.exe | Receives and/or sends multicast data as part of ... | 手动 | 正在运行 |

C、删除服务

选择可疑服务项，右键属性，停止服务，启动类型：禁止。

Remote UPnP Service 的属性 (本地计算机)

名称: RemoteUPnPService

显示名称: Remote UPnP Service

描述: Enables a common interface and object model for the Remote UPnP Service to access management information about system update, network protocols, devices and applications. If this service is stopped, most Kernel-based software will not function properly. If this service is disabled, any services that depend on it will fail to start.

启动类型 (S): 手动

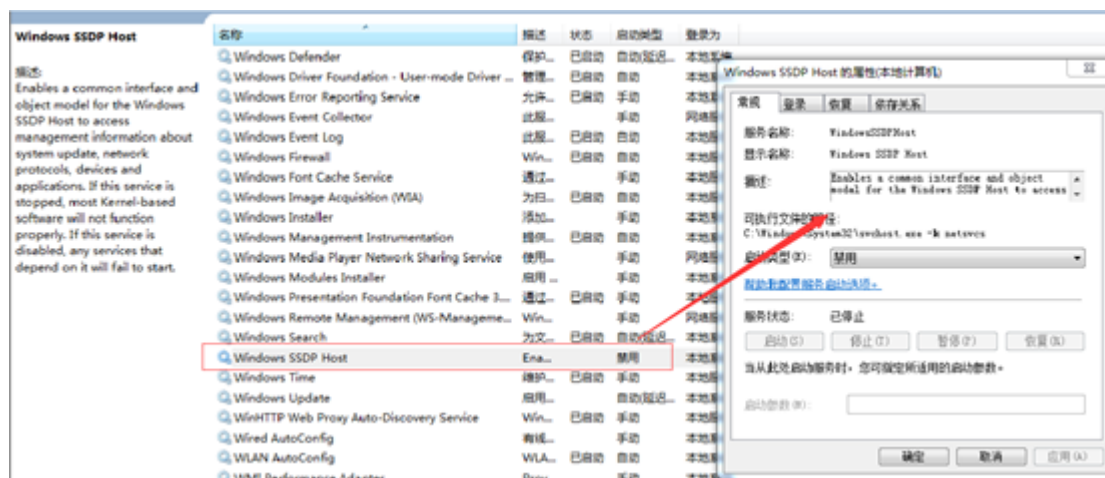
服务状态: 已停止

启动参数 (P):

确定 取消 应用 (A)

停止并禁用服务，再清除NetworkDistribution目录后，重启计算机。异常请求和目录的现象消失。

又排查了几台，现象一致，就是服务项的名称有点变化。



D、病毒清除

挖矿病毒清除过程如下：

1、停止并禁用可疑的服务项，服务项的名称会变，但描述是不变的，根据描述可快速找到可疑服务项。

可疑服务项描述：Enables a common interface and object model for the Remote UPnP Service to access

删除服务项：Sc delete RemoteUPnPService

2、删除C:\Windows\NetworkDistribution目录

3、重启计算机

4、使用杀毒软件全盘查杀

5、到微软官方网站下载对应操作系统补丁，下载链接：

<https://docs.microsoft.com/zh-cn/security-updates/securitybulletins/2017/ms17-010>

0x03 后记

在查询了大量资料后，找到了一篇在2018年2月有关该病毒的报告：

NrsMiner：一个构造精密的挖矿僵尸网络

<https://www.freebuf.com/articles/system/162874.html>

根据文章提示，这个病毒的构造非常的复杂，主控模块作为服务“Hyper-VAcess Protection Agent Service”的ServiceDll存在。但与目前处理的情况有所不同，该病毒疑似是升级了。

后续持续更新内容，将发布在公众号Bypass--，同时公众号提供了该项目的PDF版本，关注后回复“应急响应”即可下载。

