
Windows 主机入侵排查手册.md

Windows 主机入侵排查手册

一、目录

Windows 主机入侵排查手册

- 一、目录
- 二、入侵排查溯源思路
 - 1. 服务器基础情况确认
- 三、主机行为分析
 - 1. 异常文件检测
 - 2. 简易查看可疑进程
 - 3. 详细查看可疑进程及端口
 - 4. 态势感知信息复查
 - 5. 火绒剑工具使用简介
 - 6. 辅助工具
 - 7. 常见中间件日志存储位置
 - 8. 数据库日志查看
 - 9. 溯源报告撰写模板
 - 10. 参考资料

二、入侵排查溯源思路

1. 服务器基础情况确认

1. 服务器是否有 直接/ 间接 互联网应用
 - 间接互联网入侵场景：
 - A 主机收到了告警信息：A 提供了 MSSQL 数据库服务，经过与业务确认，是 xxx 系统的数据库系统，xxx 系统是在互联网应用；
 - 那么黑客可能获取了 xxx 系统的 webshell，或者通过 Sql 注入漏洞，控制了 A 的 MSSQL 数据库服务，进而获取了 A 主机的权限；
 - 路径为：互联网系统->A 主机 MSSQL 数据库->A 主机权限。
(间接)
 - 直接互联网入侵场景：

-
- B 主机收到了 webshell 告警信息：A 提供了 WEB 应用服务，经过与业务确认，xxx 系统是在互联网应用系统。黑客可能通过此系统的漏洞直接获取了 B 主机权限；
 - 路径为：互联网系统->B 主机权限。（直接）

2. 内网环境横向渗透

- 内网横向渗透场景：

- 收到告警：C 主机正在对 D,E 主机发起永恒之蓝攻击，尝试爆破 F 主机的登录密码；
- 经过与 IT 团队确认，此系统无间接/直接互联网应用（与上述情况有区分）；
- 推测：黑客可能获取了与 C 主机能够有网络通信的主机 X（未知）权限。
- 路径为：互联网系统-> X（未知）权限-> ... ->Y（未知）权限->C 主机权限。

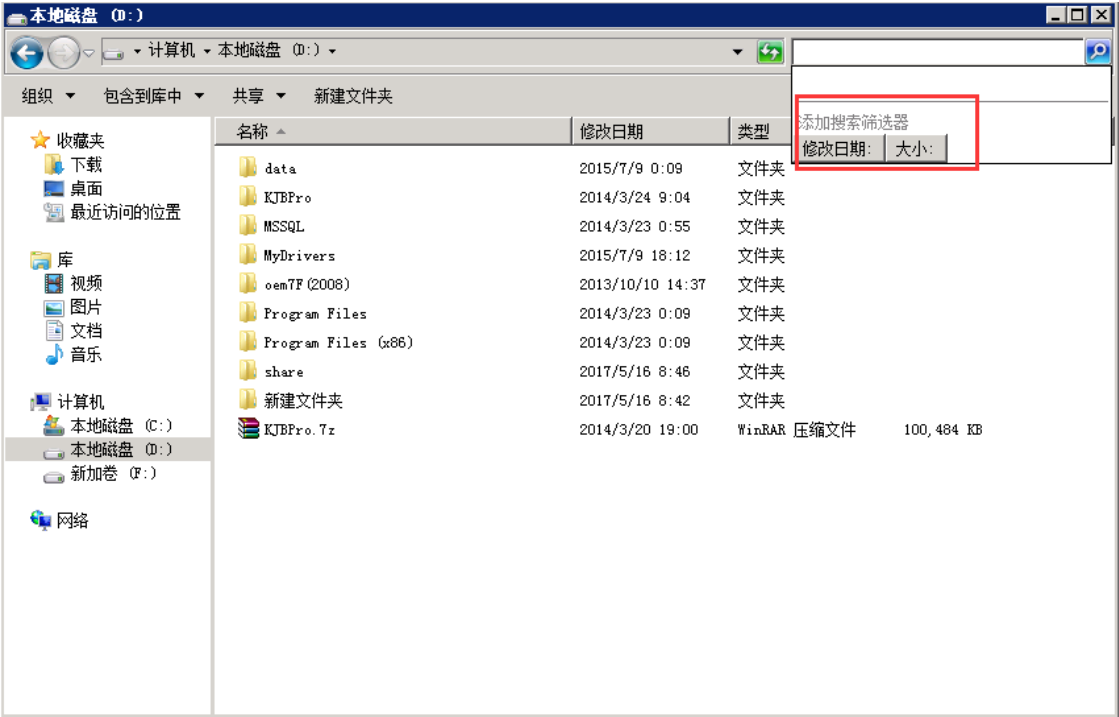
三、主机行为分析

1. 异常文件检测

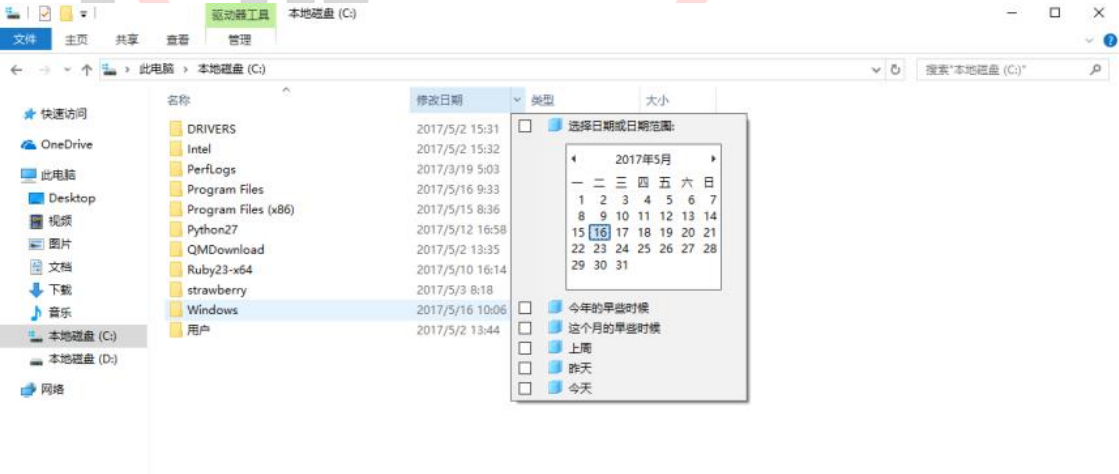
1. 开机启动有无异常文件；
2. 各个盘下的 temp(tmp)相关目录下查看有无异常文件；
3. 浏览器浏览痕迹、浏览器下载文件、浏览器 cookie 信息；
4. 查看文件时间，创建时间、修改时间、访问时间。对应 linux 的 ctime mtime atime，通过对文件右键属性即可看到详细的时间（也可以通过 dir /tc 1.aspx 来查看创建时间），黑客通过菜刀类工具改变的是修改时间。所以如果修改时间在创建时间之前明显是可疑文件；
5. 查看用户 recent 相关文件，通过分析最近打开分析可疑文件：
 - C:\Documents and Settings\Administrator\Recent
 - C:\Documents and Settings\Default User\Recent
 - 开始，运行 %UserProfile%\Recent

6. 根据文件夹内文件列表时间进行排序，查找可疑文件。当然也可以搜索指定日期范围的文件及文件；

– 示例：Server 2008 R2 系列



– 示例：Win10 系列



7. 关键字匹配，通过确定后的入侵时间，以及 webshell 或 js 文件的关键字（比如博彩类），可以在 IIS 日志中进行过滤匹配，比如经常使用：

知道是上传目录，在 web log 中查看指定时间范围包括上传文件夹的访问请求
findstr /s /m /I "UploadFiles" *.log
某次博彩事件中的六合彩信息是 six.js
findstr /s /m /I "six.js" *.aspx
根据 shell 名关键字去搜索 D 盘 spy 相关的文件有哪些
for /r d:\ %i in (*spy*.aspx) do @echo %i

2. 简易查看可疑进程

1. netstat -ano 查看目前的网络连接，定位可疑的 ESTABLISHED
2. 根据 netstat 定位出的 pid，再通过 tasklist 命令进行进程定位
3. 例如：

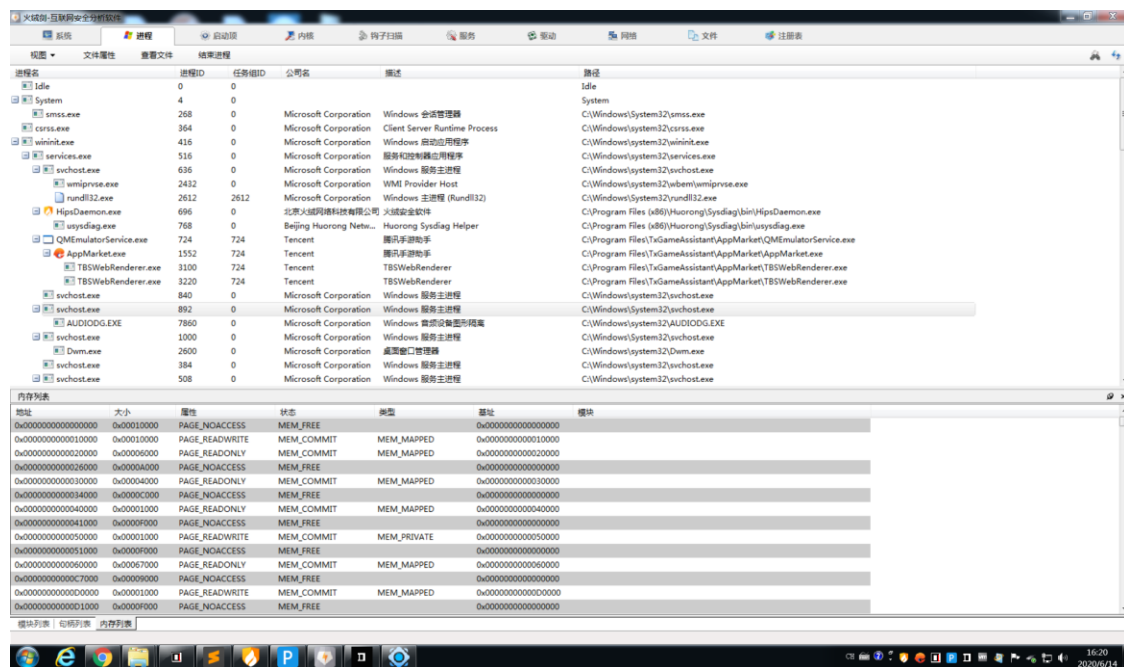
```
C:\Users\sm0nk>netstat -ano | findstr ESTABLISHED
TCP    127.0.0.1:443          127.0.0.1:12844      ESTABLISHED 5316
TCP    127.0.0.1:443          127.0.0.1:12868      ESTABLISHED 5316
TCP    127.0.0.1:443          127.0.0.1:12869      ESTABLISHED 5316
TCP    127.0.0.1:443          127.0.0.1:12870      ESTABLISHED 5316
TCP    127.0.0.1:1975         127.0.0.1:1976       ESTABLISHED 8
TCP    127.0.0.1:1976         127.0.0.1:1975       ESTABLISHED 8
TCP    127.0.0.1:2271         127.0.0.1:2272       ESTABLISHED 5316
TCP    127.0.0.1:2272         127.0.0.1:2271       ESTABLISHED 5316
TCP    127.0.0.1:12844        127.0.0.1:443         ESTABLISHED 12992
TCP    127.0.0.1:12845        127.0.0.1:12846       ESTABLISHED 12992
TCP    127.0.0.1:12846        127.0.0.1:12845       ESTABLISHED 12992
TCP    127.0.0.1:12868        127.0.0.1:443         ESTABLISHED 12992
TCP    127.0.0.1:12869        127.0.0.1:443         ESTABLISHED 12992
TCP    127.0.0.1:12870        127.0.0.1:443         ESTABLISHED 12992
TCP    192.168.1.102:2089     180.163.21.35:80      ESTABLISHED 1444
TCP    192.168.1.102:2465     192.168.3.141:445     ESTABLISHED 4
TCP    192.168.1.102:2492     192.168.3.143:22      ESTABLISHED 8548
TCP    192.168.1.102:6427     23.79.16.113:443      ESTABLISHED 10404
TCP    192.168.1.102:6614     111.221.29.75:443     ESTABLISHED 4052
TCP    192.168.1.102:7259     101.227.162.139:80    ESTABLISHED 6696
TCP    192.168.1.102:12410    52.41.66.130:443      ESTABLISHED 8
TCP    192.168.1.102:12877    23.33.164.43:443      ESTABLISHED 12992
TCP    192.168.1.102:13211    14.17.42.118:80       ESTABLISHED 8
TCP    192.168.1.102:13214    101.226.99.117:80     ESTABLISHED 6696
TCP    [::1]:8307             [::1]:12849           ESTABLISHED 5316
TCP    [::1]:8307             [::1]:12871           ESTABLISHED 5316
TCP    [::1]:8307             [::1]:12872           ESTABLISHED 5316
TCP    [::1]:8307             [::1]:12873           ESTABLISHED 5316
TCP    [::1]:12849            [::1]:8307            ESTABLISHED 5316
TCP    [::1]:12871            [::1]:8307            ESTABLISHED 5316
TCP    [::1]:12872            [::1]:8307            ESTABLISHED 5316
TCP    [::1]:12873            [::1]:8307            ESTABLISHED 5316

C:\Users\sm0nk>tasklist /svc | findstr 10404
WinStore.App.exe    10404 暂缺
```

- 4.
5. img

3. 详细查看可疑进程及端口

1. 通过火绒剑的网络，进程，系统或者 **PCHunter** 的网络完成分析（请注意手动刷新）
 - 火绒剑下载地址：<https://www.huorong.cn/person5.html>
 - PC Hunter 下载地址：<http://www.xuetr.com/>
2. 火绒剑分析工具使用示例：



4. 态势感知信息复查

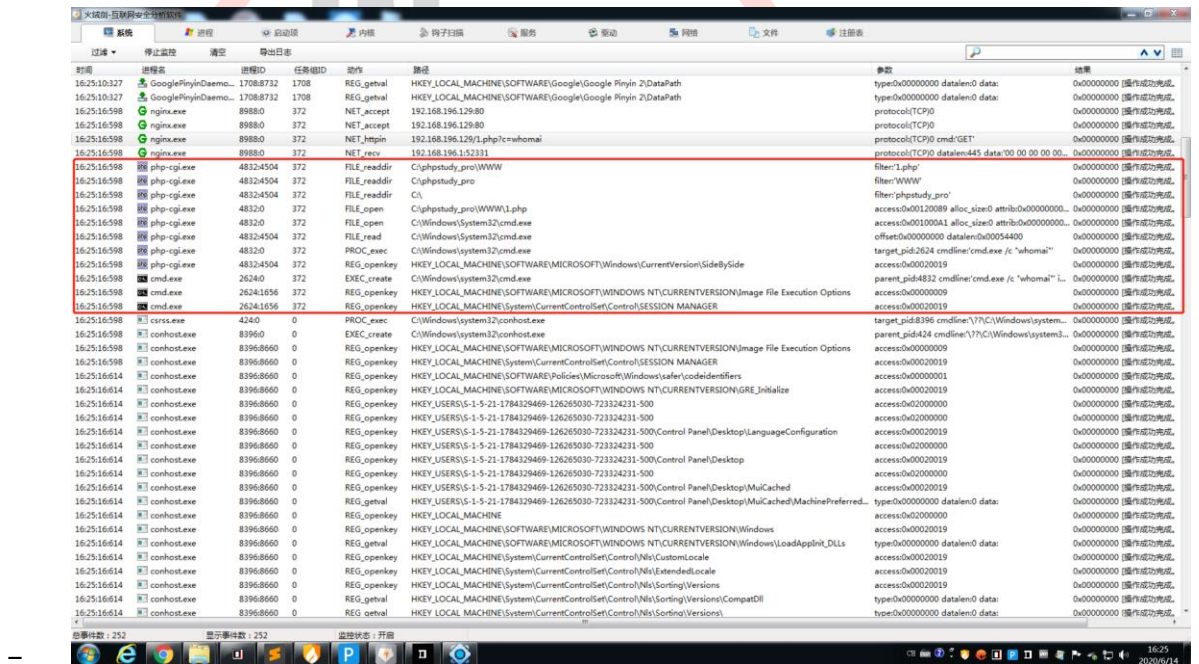
1. 若态势感知相关工具发生告警，重点检查如下几点，确认入侵者影响范围：
 - 若入侵者获取到的系统权限
 - 当前用户 query
 - 查询是否有隐藏用户
 - 查询系统用户登录日志
 - 查看用户最近访问情况:%UserProfile%\Recent
 - 若入侵者仅获取到 shell 权限：

- 重点分析对应的 web 日志
- 若入侵者仅获取到数据库权限：
 - udf.dll
 - run_java
 - xp_cmdshell

5. 火绒剑工具使用简介

1. 监控是否有异常进程，示例

- 图中：监测到 whomai 的命令执行，攻击入口为 `http://192.168.196.129/1.php?c=whomai`，攻击源 ip 为 192.168.196.1



2. 监控是否有异常网络连接，示例：

- 监测到 tcp.exe 与 47.98.164.103 的 8888 端口通信异常；

属性	结束进程	查看文件	安全状态	模块	协议	本地地址	远程地址	状态
61.168.100.225								
Idle	0	系统文件			TCP	192.168.196.129:49765	61.168.100.225:80	TS_time_wait
Idle	0	系统文件			TCP	192.168.196.129:49766	61.168.100.225:80	TS_time_wait
Idle	0	系统文件			TCP	192.168.196.129:49767	61.168.100.225:80	TS_time_wait
Idle	0	系统文件			TCP	192.168.196.129:49768	61.168.100.225:80	TS_time_wait
Idle	0	系统文件			TCP	192.168.196.129:49769	61.168.100.225:80	TS_time_wait
Idle	0	系统文件			TCP	192.168.196.129:49770	61.168.100.225:80	TS_time_wait
Idle	0	系统文件			TCP	192.168.196.129:49771	61.168.100.225:80	TS_time_wait
Idle	0	系统文件			TCP	192.168.196.129:49772	61.168.100.225:80	TS_time_wait
Idle	0	系统文件			TCP	192.168.196.129:49773	61.168.100.225:80	TS_time_wait
Idle	0	系统文件			TCP	192.168.196.129:49774	61.168.100.225:80	TS_time_wait
58.347.205.183								
AppMarket.exe	1552	数字签名文件		C:\Program Files\Tencent\GameAssistant\GameMarketA...	TCP	192.168.196.129:49752	58.347.205.183:80	TS_close_wait
AppMarket.exe	1552	数字签名文件		C:\Program Files\Tencent\GameAssistant\GameMarketA...	TCP	192.168.196.129:49753	58.347.205.183:80	TS_close_wait
AppMarket.exe	1552	数字签名文件		C:\Program Files\Tencent\GameAssistant\GameMarketA...	TCP	192.168.196.129:49754	58.347.205.183:80	TS_close_wait
47.98.164.103								
XshellCore.exe	5828	数字签名文件		C:\Users\Administrator\Desktop\Backup\Xshell_P...	TCP	192.168.196.129:49650	47.98.164.103:22	TS_established
tcp.exe	23092	未知文件		C:\Users\Administrator\Desktop\tcp.exe	TCP	192.168.196.129:49780	47.98.164.103:8888	TS_sync_sent
203.208.50.98								
chrome.exe	1652	数字签名文件		C:\Program Files (x86)\Google\Chrome\Applicati...	TCP	192.168.196.129:49470	203.208.50.98:443	TS_close_wait
127.0.0.1								
gwsupdater.exe	1844	数字签名文件		C:\Program Files (x86)\Gateway\SSVPN\gwsupda...	TCP	127.0.0.1:49161	127.0.0.1:49162	TS_established
gwsupdater.exe	1844	数字签名文件		C:\Program Files (x86)\Gateway\SSVPN\gwsupda...	TCP	127.0.0.1:49162	127.0.0.1:49161	TS_established
gwsupdater.exe	1844	数字签名文件		C:\Program Files (x86)\Gateway\SSVPN\gwsupda...	TCP	127.0.0.1:49163	127.0.0.1:49164	TS_established
gwsupdater.exe	1844	数字签名文件		C:\Program Files (x86)\Gateway\SSVPN\gwsupda...	TCP	127.0.0.1:49164	127.0.0.1:49163	TS_established
gwservice.exe	1748	数字签名文件		C:\Program Files (x86)\Gateway\SSVPN\gwserv...	TCP	127.0.0.1:49166	127.0.0.1:49167	TS_established
gwservice.exe	1748	数字签名文件		C:\Program Files (x86)\Gateway\SSVPN\gwserv...	TCP	127.0.0.1:49167	127.0.0.1:49166	TS_established
gwservice.exe	1748	数字签名文件		C:\Program Files (x86)\Gateway\SSVPN\gwserv...	TCP	127.0.0.1:49168	127.0.0.1:49169	TS_established
gwservice.exe	1748	数字签名文件		C:\Program Files (x86)\Gateway\SSVPN\gwserv...	TCP	127.0.0.1:49169	127.0.0.1:49168	TS_established
0.0.0.0								
TeamViewer_Service.exe	2024	数字签名文件		C:\Program Files (x86)\TeamViewer\TeamViewe...	TCP	127.0.0.1:5939	0.0.0.0	TS_listen
gwsupdater.exe	1844	数字签名文件		C:\Program Files (x86)\Gateway\SSVPN\gwsupda...	TCP	127.0.0.1:36000	0.0.0.0	TS_listen
gwsupdater.exe	1844	数字签名文件		C:\Program Files (x86)\Gateway\SSVPN\gwsupda...	TCP	127.0.0.1:36001	0.0.0.0	TS_listen
gwsupdater.exe	1844	数字签名文件		C:\Program Files (x86)\Gateway\SSVPN\gwsupda...	TCP	127.0.0.1:36002	0.0.0.0	TS_listen
gwsupdater.exe	1844	数字签名文件		C:\Program Files (x86)\Gateway\SSVPN\gwsupda...	TCP	127.0.0.1:36003	0.0.0.0	TS_listen
gwsupdater.exe	1844	数字签名文件		C:\Program Files (x86)\Gateway\SSVPN\gwsupda...	TCP	127.0.0.1:36004	0.0.0.0	TS_listen
gwsupdater.exe	1844	数字签名文件		C:\Program Files (x86)\Gateway\SSVPN\gwsupda...	TCP	127.0.0.1:36005	0.0.0.0	TS_listen

3. 查看异常启动项、服务、计划任务

- 注意观察图中未知文件

名称	安全状态	描述	公司名	路径
Narrator	系统文件	Narrator	Microsoft Corporation	C:\Windows\System32\Narrator.exe
Oracle_JavaAccessBrid...	数字签名文件	Java(TM) Platform SE binary	Oracle Corporation	C:\Program Files\Java\jre1.8.0_251\bin\java.exe
osk	系统文件	辅助功能屏幕键盘	Microsoft Corporation	C:\Windows\System32\osk.exe
magflap.exe	未知文件	Microsoft 屏幕放大	Microsoft Corporation	C:\Windows\System32\Magnify.exe
Narrator	系统文件	Narrator	Microsoft Corporation	C:\Windows\System32\Narrator.exe
osk	系统文件	辅助功能屏幕键盘	Microsoft Corporation	C:\Windows\System32\osk.exe
KEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SafeBoot				
cmd.exe	系统文件	Windows 命令提示符	Microsoft Corporation	C:\Windows\system32\cmd.exe
ProgramData\Microsoft\Windows\Start Menu\Programs\Startup				
tcp.exe - 快速方式链接	未知文件			C:\Users\Administrator\Desktop\tcp.exe
application\octet-stream	系统文件	Microsoft .NET Runtime Execut...	Microsoft Corporation	C:\Windows\system32\mscexec.dll
application/x-complex	系统文件	Microsoft .NET Runtime Execut...	Microsoft Corporation	C:\Windows\system32\mscexec.dll
application/x-msdownl...	系统文件	Microsoft .NET Runtime Execut...	Microsoft Corporation	C:\Windows\system32\mscexec.dll
KEY_CLASSES_ROOT\PROTOCOLS\Handler				
about	系统文件	Microsoft (R) HTML 查看器	Microsoft Corporation	C:\Windows\System32\mshtml.dll
cdll	系统文件	Win32 的 OLE32 扩展	Microsoft Corporation	C:\Windows\system32\urlmon.dll
dvd	系统文件	ActiveX 的 ActiveX 控件	Microsoft Corporation	C:\Windows\system32\msvidctl.dll
file	系统文件	Win32 的 OLE32 扩展	Microsoft Corporation	C:\Windows\system32\urlmon.dll
ftp	系统文件	Win32 的 OLE32 扩展	Microsoft Corporation	C:\Windows\system32\urlmon.dll
http	系统文件	Win32 的 OLE32 扩展	Microsoft Corporation	C:\Windows\system32\urlmon.dll
https	系统文件	Win32 的 OLE32 扩展	Microsoft Corporation	C:\Windows\system32\urlmon.dll
its	系统文件	Microsoft? InfoTech Storage Sy...	Microsoft Corporation	C:\Windows\System32\its.dll
javascript	系统文件	Microsoft (R) HTML 查看器	Microsoft Corporation	C:\Windows\System32\mshtml.dll
local	系统文件	Win32 的 OLE32 扩展	Microsoft Corporation	C:\Windows\system32\urlmon.dll
mailto	系统文件	Microsoft (R) HTML 查看器	Microsoft Corporation	C:\Windows\System32\mshtml.dll
mhmtl	系统文件	Microsoft Internet Messaging A...	Microsoft Corporation	C:\Windows\system32\inetcomm.dll
mk	系统文件	Win32 的 OLE32 扩展	Microsoft Corporation	C:\Windows\system32\urlmon.dll
ms-its	系统文件	Microsoft? InfoTech Storage Sy...	Microsoft Corporation	C:\Windows\System32\its.dll
res	系统文件	Microsoft (R) HTML 查看器	Microsoft Corporation	C:\Windows\System32\mshtml.dll
tv	系统文件	ActiveX 的 ActiveX 控件	Microsoft Corporation	C:\Windows\System32\msvidctl.dll
vbscript	系统文件	Microsoft (R) HTML 查看器	Microsoft Corporation	C:\Windows\System32\mshtml.dll
模块:		tcp.exe		
路径:		C:\Users\Administrator\Desktop\tcp.exe		
备注说明:				
版本:				
公司:				

6. 辅助工具

1. 可采用 D 盾作为辅助工具快速检查系统异常：

- 下载地址：<http://www.d99net.net/>
- 示例：



7. 常见中间件日志存储位置

1. apache 的日志路径一般配置在 httpd.conf
2. IIS 的日志默认在系统目录下的 Logfiles 下的目录当中
3. tomcat 一般位于 tomcat 安装目录下的一个 logs 文件夹下面
4. Nginx 日志一般配置在 nginx.conf 或者 vhost 的 conf 文件中

8. 数据库日志查看

1. 查看数据库登陆相关日志，如 mssql, oracle, mysql
2. 示例：

10. 参考资料

- [Windows 应急响应指南](#)
- [windows-应急流程及实战演练\(FTP 暴力破解, 蠕虫, 勒索病毒\)](#)
- [7.11. 应急响应— Web 安全学习笔记 1.0 文档](#)
- [应急响应资料整理](#)
- [\[比敌人更了解敌人 \[取证入门 web 篇\]](#)
- [黑客入侵应急分析手工排查](#)
- [HW 防守 | Windows 应急响应基础](#)
- [通过服务器日志溯源定位 web 应用攻击路径](#)
- [捕获一起恶意入侵事件的攻击溯源](#)

