第2篇：蠕虫病毒

0x00 前言

蠕虫病毒是一种十分古老的计算机病毒，它是一种自包含的程序（或是一套程序），通常通过网络途径传播，每入侵到一台新的计算机，它就在这台计算机上复制自己，并自动执行它自身的程序。

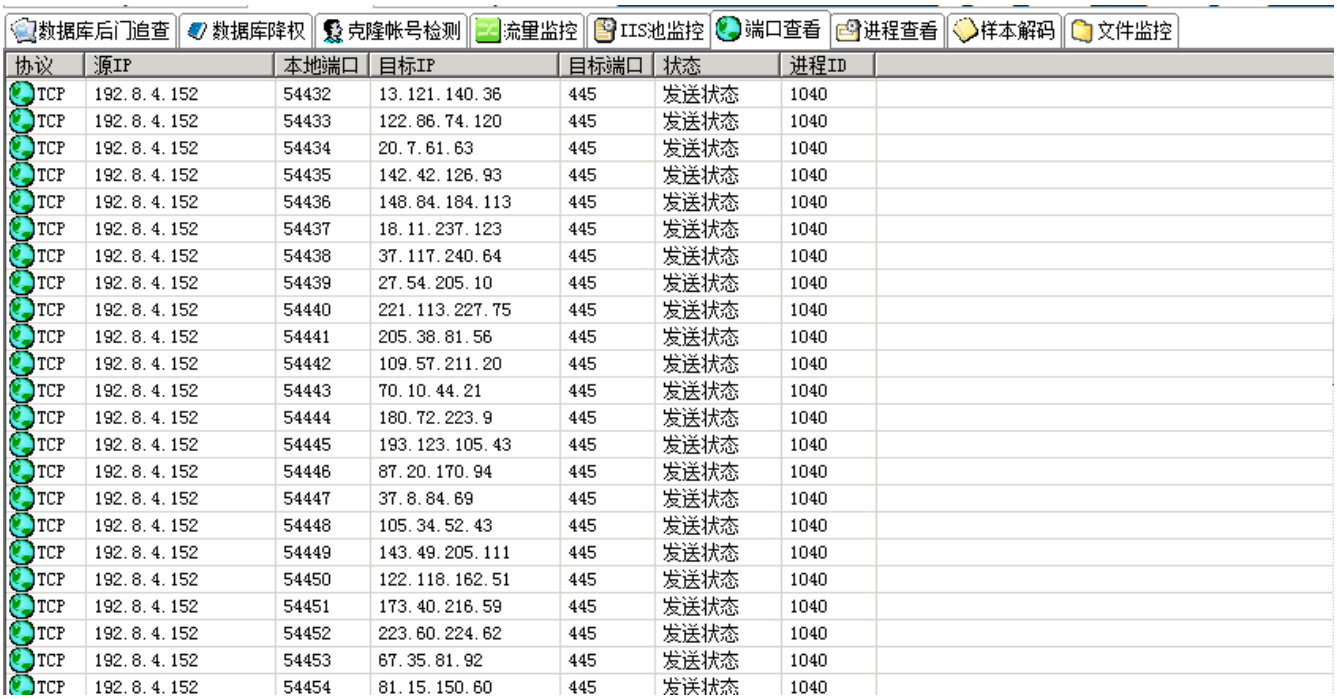
常见的蠕虫病毒：熊猫烧香病毒 、冲击波/震荡波病毒、conficker病毒等。

0x01 应急场景

某天早上，管理员在出口防火墙发现内网服务器不断向境外IP发起主动连接，内网环境，无法连通外网，无图脑补。

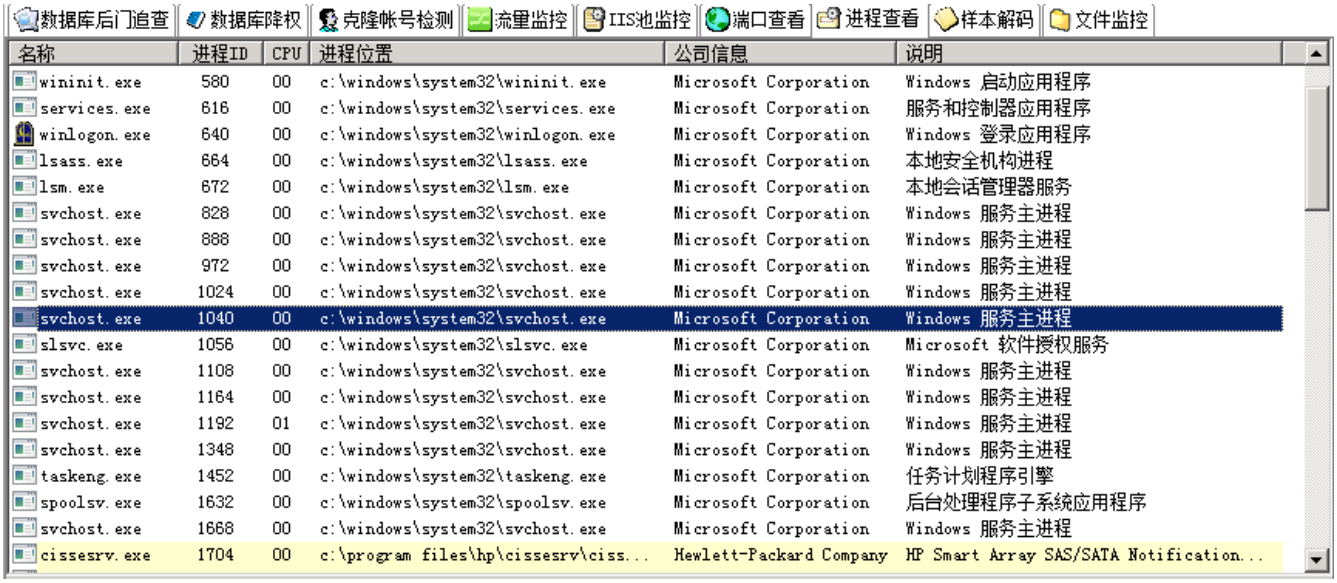
0x02 事件分析

在出口防火墙看到的服务器内网IP，首先将中病毒的主机从内网断开，然后登录该服务器，打开D盾_web查杀查看端口连接情况，可以发现本地向外网IP发起大量的主动连接：



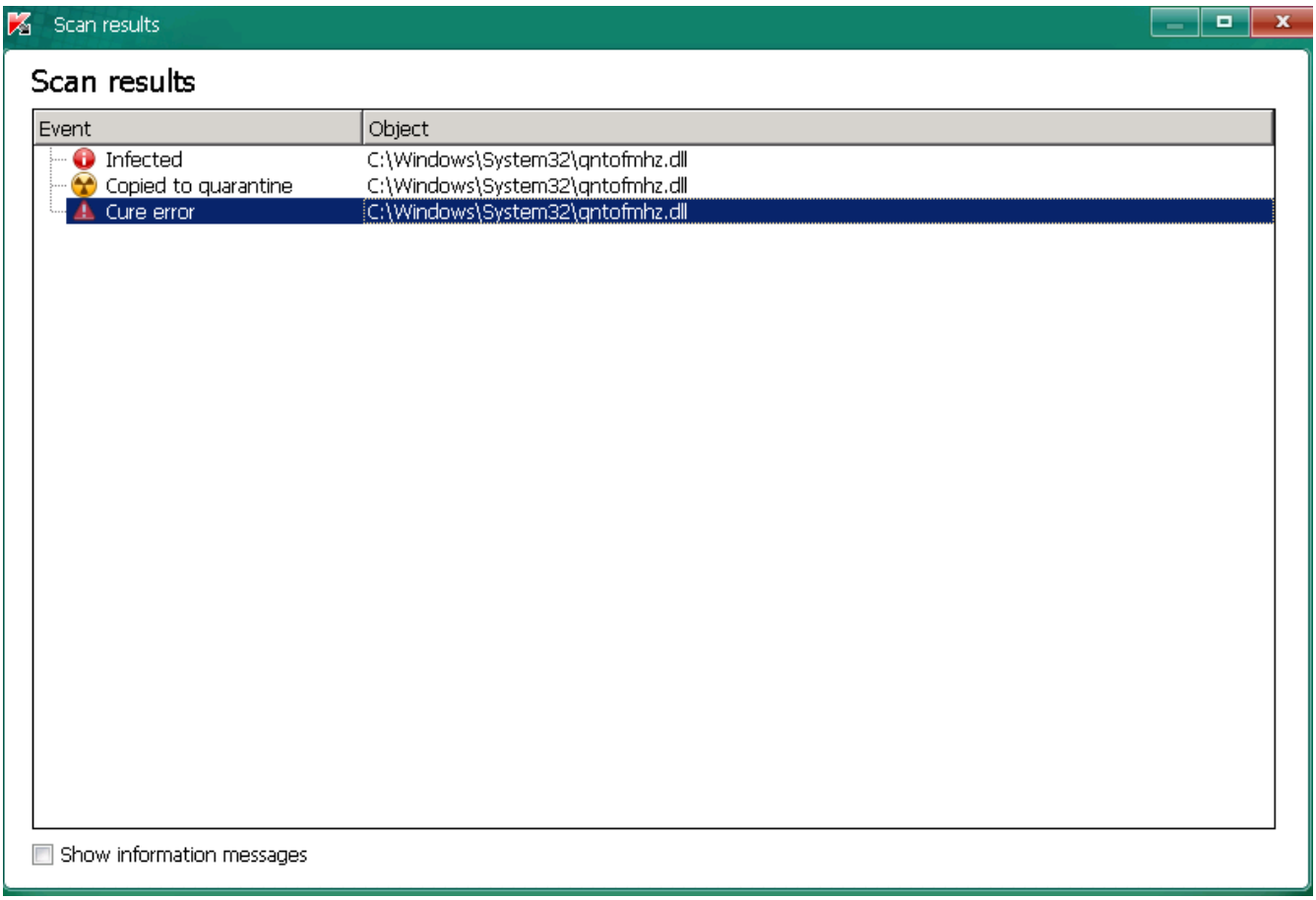
协议	源IP	本地端口	目标IP	目标端口	状态	进程ID
TCP	192.8.4.152	54432	13.121.140.36	445	发送状态	1040
TCP	192.8.4.152	54433	122.86.74.120	445	发送状态	1040
TCP	192.8.4.152	54434	20.7.61.63	445	发送状态	1040
TCP	192.8.4.152	54435	142.42.126.93	445	发送状态	1040
TCP	192.8.4.152	54436	148.84.184.113	445	发送状态	1040
TCP	192.8.4.152	54437	18.11.237.123	445	发送状态	1040
TCP	192.8.4.152	54438	37.117.240.64	445	发送状态	1040
TCP	192.8.4.152	54439	27.54.205.10	445	发送状态	1040
TCP	192.8.4.152	54440	221.113.227.75	445	发送状态	1040
TCP	192.8.4.152	54441	205.38.81.56	445	发送状态	1040
TCP	192.8.4.152	54442	109.57.211.20	445	发送状态	1040
TCP	192.8.4.152	54443	70.10.44.21	445	发送状态	1040
TCP	192.8.4.152	54444	180.72.223.9	445	发送状态	1040
TCP	192.8.4.152	54445	193.123.105.43	445	发送状态	1040
TCP	192.8.4.152	54446	87.20.170.94	445	发送状态	1040
TCP	192.8.4.152	54447	37.8.84.69	445	发送状态	1040
TCP	192.8.4.152	54448	105.34.52.43	445	发送状态	1040
TCP	192.8.4.152	54449	143.49.205.111	445	发送状态	1040
TCP	192.8.4.152	54450	122.118.162.51	445	发送状态	1040
TCP	192.8.4.152	54451	173.40.216.59	445	发送状态	1040
TCP	192.8.4.152	54452	223.60.224.62	445	发送状态	1040
TCP	192.8.4.152	54453	67.35.81.92	445	发送状态	1040
TCP	192.8.4.152	54454	81.15.150.60	445	发送状态	1040

通过端口异常，跟踪进程ID，可以找到该异常由svchost.exe windows服务主进程引起，svchost.exe向大量远程IP的445端口发送请求：



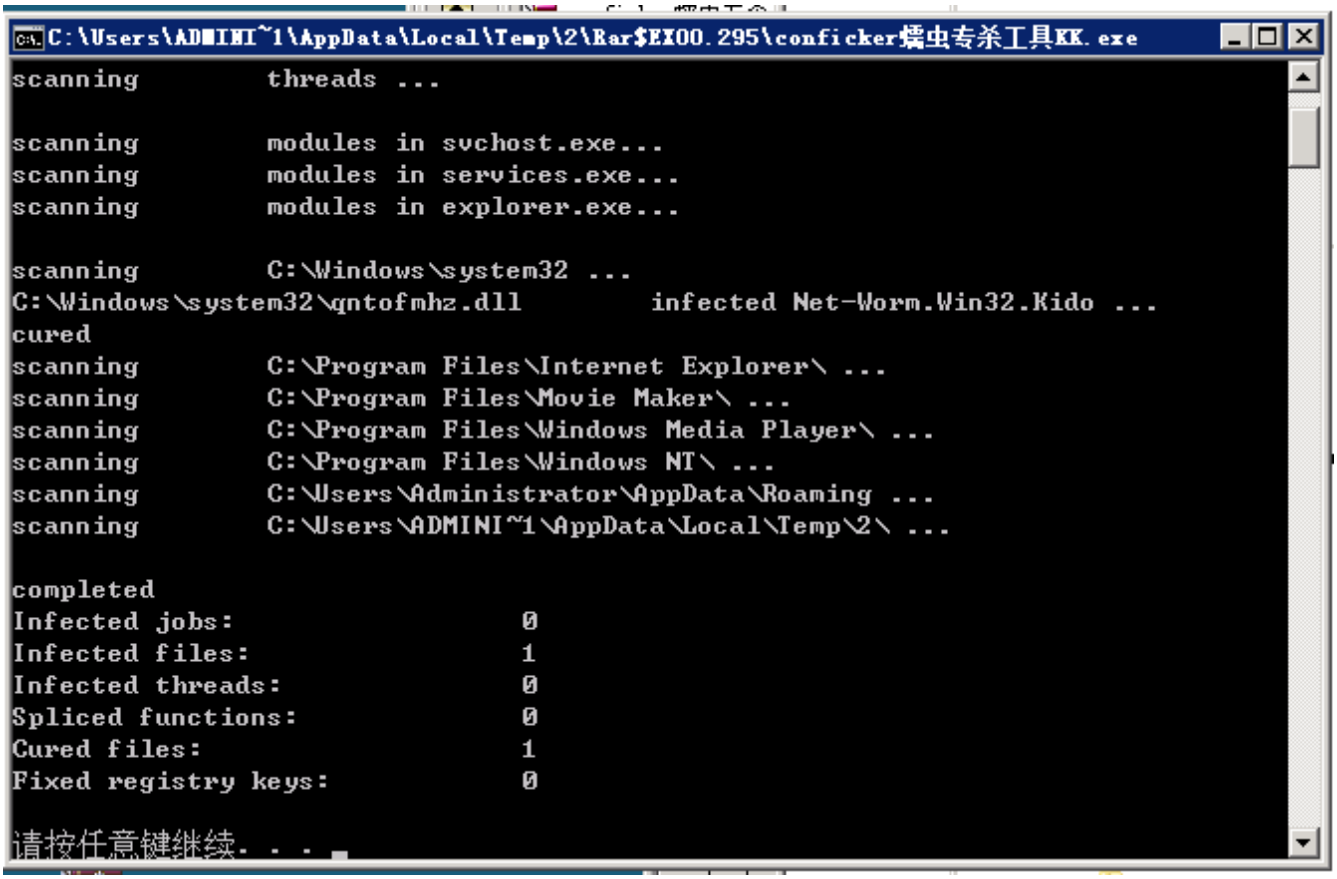
名称	进程ID	CPU	进程位置	公司信息	说明
wininit.exe	580	00	c:\windows\system32\wininit.exe	Microsoft Corporation	Windows 启动应用程序
services.exe	616	00	c:\windows\system32\services.exe	Microsoft Corporation	服务和控制器应用程序
winlogon.exe	640	00	c:\windows\system32\winlogon.exe	Microsoft Corporation	Windows 登录应用程序
lsass.exe	664	00	c:\windows\system32\lsass.exe	Microsoft Corporation	本地安全机构进程
lsm.exe	672	00	c:\windows\system32\lsm.exe	Microsoft Corporation	本地会话管理器服务
svchost.exe	828	00	c:\windows\system32\svchost.exe	Microsoft Corporation	Windows 服务主进程
svchost.exe	888	00	c:\windows\system32\svchost.exe	Microsoft Corporation	Windows 服务主进程
svchost.exe	972	00	c:\windows\system32\svchost.exe	Microsoft Corporation	Windows 服务主进程
svchost.exe	1024	00	c:\windows\system32\svchost.exe	Microsoft Corporation	Windows 服务主进程
svchost.exe	1040	00	c:\windows\system32\svchost.exe	Microsoft Corporation	Windows 服务主进程
slsvc.exe	1056	00	c:\windows\system32\slsvc.exe	Microsoft Corporation	Microsoft 软件授权服务
svchost.exe	1108	00	c:\windows\system32\svchost.exe	Microsoft Corporation	Windows 服务主进程
svchost.exe	1164	00	c:\windows\system32\svchost.exe	Microsoft Corporation	Windows 服务主进程
svchost.exe	1192	01	c:\windows\system32\svchost.exe	Microsoft Corporation	Windows 服务主进程
svchost.exe	1348	00	c:\windows\system32\svchost.exe	Microsoft Corporation	Windows 服务主进程
taskeng.exe	1452	00	c:\windows\system32\taskeng.exe	Microsoft Corporation	任务计划程序引擎
spoolsv.exe	1632	00	c:\windows\system32\spoolsv.exe	Microsoft Corporation	后台处理程序子系统应用程序
svchost.exe	1668	00	c:\windows\system32\svchost.exe	Microsoft Corporation	Windows 服务主进程
cissesrv.exe	1704	00	c:\program files\hp\cissesrv\ciss...	Hewlett-Packard Company	HP Smart Array SAS/SATA Notification...

这里我们推测可以系统进程被病毒感染，使用卡巴斯基病毒查杀工具，对全盘文件进行查杀，发现c:\windows\system32\qntofmhz.dll异常：



使用多引擎在线病毒扫描（http://www.virscan.org/） 对该文件进行扫描:

确认服务器感染conficker蠕虫病毒，下载conficker蠕虫专杀工具对服务器进行清查，成功清楚病毒。



大致的处理流程如下:

1、发现异常：出口防火墙、本地端口连接情况，主动向外网发起大量连接
2、病毒查杀：卡巴斯基全盘扫描，发现异常文件
3、确认病毒：使用多引擎在线病毒对该文件扫描，确认服务器感染conficker蠕虫病毒。
4、病毒处理：使用conficker蠕虫专杀工具对服务器进行清查，成功清除病毒。

0x04 预防处理措施

在政府、医院内网，依然存在着一些很古老的感染性病毒，如何保护电脑不受病毒感染，总结了几种预防措施：

1、安装杀毒软件，定期全盘扫描
2、不使用来历不明的软件，不随意接入未经查杀的U盘
3、定期对windows系统漏洞进行修复，不给病毒可乘之机
4、做好重要文件的备份，备份，备份。

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。