windows 应急流程及实战演练

当企业发生黑客入侵、系统崩溃或其它影响业务正常运行的安全事件时，急需第一时间进行处理，使企业的网络信息系统在最短时间内恢复正常工作，进一步查找入侵来源，还原入侵事故过程，同时给出解决方案与防范措施，为企业挽回或减少经济损失。

常见的应急响应事件分类：

web 入侵：网页挂马、主页篡改、Webshell

系统入侵：病毒木马、勒索软件、远控后门

网络攻击：DDOS 攻击、DNS 劫持、ARP 欺骗

针对常见的攻击事件，结合工作中应急响应事件分析和解决的方法，总结了一些 Window 服务器入侵排查的思路。

0x01 入侵排查思路

一、检查系统账号安全

1、查看服务器是否有弱口令，远程管理端口是否对公网开放。

检查方法：

据实际情况咨询相关服务器管理员。

2、查看服务器是否存在可疑账号、新增账号。

检查方法：

打开 cmd 窗口，输入 `lusrmgr.msc` 命令，查看是否有新增/可疑的账号，如有管理员群组的（Administrators）里的新增账户，如有，请立即禁用或删除掉。

3、查看服务器是否存在隐藏账号、克隆账号。

检查方法：

a、打开注册表，查看管理员对应键值。

b、使用 D 盾 _web 查杀工具，集成了对克隆账号检测的功能。

4、结合日志，查看管理员登录时间、用户名是否存在异常。

检查方法：

a、Win+R 打开运行，输入“eventvwr.msc”，回车运行，打开“事件查看器”。

b、导出 Windows 日志--安全，利用 Log Parser 进行分析。

```
C:\Program Files (x86)\Log Parser 2.2>LogParser.exe -i:EVT "SELECT TimeGenera
 as LoginTime,EXTRACT_TOKEN(Strings,5,'|') as username FROM c:\11.evtx where
ntID=4624"
LoginTime           username
------------------- -------------
2018-06-17 18:26:24 Administrator
2018-06-17 18:54:37 SYSTEM
2018-06-18 01:21:30 Administrator
2018-06-18 01:21:39 Administrator

Statistics:
-----------
Elements processed: 9936
Elements output:    4
Execution time:     0.17 seconds
```

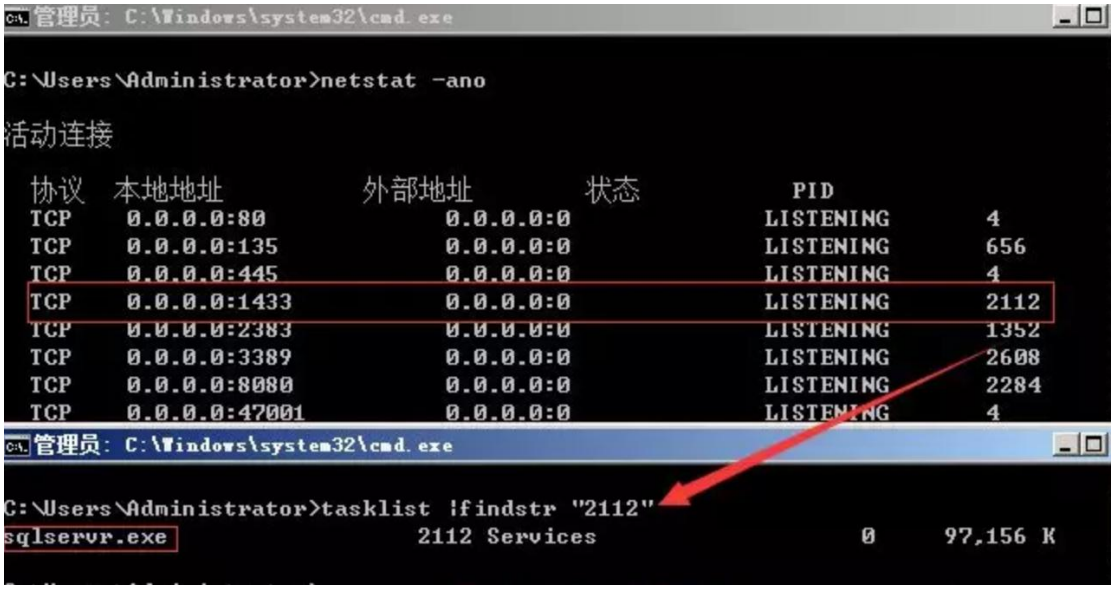
二、检查异常端口、进程

1、检查端口连接情况，是否有远程连接、可疑连接。

检查方法：

a、netstat -ano 查看目前的网络连接，定位可疑的 ESTABLISHED

b、根据 netstat 定位出的 pid，再通过 tasklist 命令进行进程定位 `tasklist | findstr "PID"`



2、进程

检查方法：

a、开始--运行--输入 `msinfo32`，依次点击“软件环境→正在运行任务”就可以查看到进程的详细信息，比如进程路径、进程 ID、文件创建日期、启动时间等。

b、打开 D 盾 _web 查杀工具，进程查看，关注没有签名信息的进程。

c、通过微软官方提供的 Process Explorer 等工具进行排查 。

d、查看可疑的进程及其子进程。可以通过观察以下内容：

- 没有签名验证信息的进程
- 没有描述信息的进程
- 进程的属主
- 进程的路径是否合法
- CPU 或内存资源占用长时间过高的进程

3、小技巧：

a、查看端口对应的 PID： `netstat -ano | findstr "port"`

b、查看进程对应的 PID：任务管理器--查看--选择列--PID 或者 `tasklist | findstr "PID"`

c、查看进程对应的程序位置：

- 任务管理器--选择对应进程--右键打开文件位置
- 运行输入 wmic，cmd 界面 输入 process

d、`tasklist /svc` 进程-- PID --服务

e、查看 Windows 服务所对应的端口：

`%system%/system32/drivers/etc/services`（一般 `%system%`就是 C:\Windows）

三、检查启动项、计划任务、服务

1、检查服务器是否有异常的启动项。

检查方法：

a、登录服务器，单击【开始】>【所有程序】>【启动】，默认情况下此目录在是一个空目录，确认是否有非业务程序在该目录下。

b、单击开始菜单 >【运行】，输入 msconfig，查看是否存在命名异常的启动项目，是则取消勾选命名异常的启动项目，并到命令中显示的路径删除文件。

c、单击【开始】>【运行】，输入 regedit，打开注册表，查看开机启动项是否正常，特别注意如下三个注册表项：

HKEY_CURRENT_USER\software\micorsoft\windows\currentversion\run

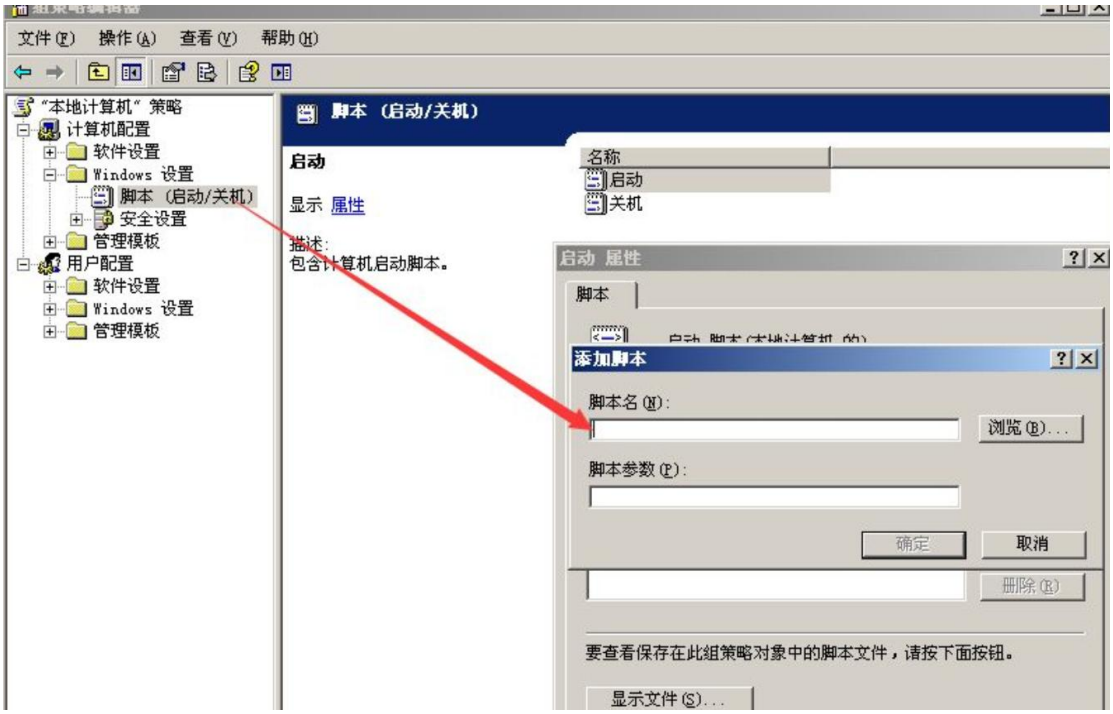
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce

检查右侧是否有启动异常的项目，如有请删除，并建议安装杀毒软件进行病毒查杀，清除残留病毒或木马。

d、利用安全软件查看启动项、开机时间管理等。

e、组策略，运行 gpedit.msc。



2、检查计划任务

检查方法：

a、单击【开始】>【设置】>【控制面板】>【任务计划】，查看计划任务属性，便可以发现木马文件的路径。

b、单击【开始】>【运行】，输入 cmd，然后输入 at，检查计算机与网络上的其它计算机之间的会话或计划任务，如有，则确认是否为正常连接。

3、服务自启动

检查方法：

单击【开始】>【运行】，输入 services.msc，注意服务状态和启动类型，检查是否有异常服务。

四、检查系统相关信息

1、查看系统版本以及补丁信息

检查方法：

单击【开始】>【运行】，输入 systeminfo，查看系统信息

2、查找可疑目录及文件

检查方法：

a、 查看用户目录，新建账号会在这个目录生成一个用户目录，查看是否有新建用户目录。

Window 2003：

C:\Documents and Settings
Window 2008R2：
C:\Users\

b、单击【开始】>【运行】，输入 `%UserProfile%\Recent`，分析最近打开分析可疑文件。

c、在服务器各个目录，可根据文件夹内文件列表时间进行排序，查找可疑文件。

五、自动化查杀

病毒查杀

检查方法：

下载安全软件，更新最新病毒库，进行全盘扫描。

webshell 查杀

检查方法：

选择具体站点路径进行 webshell 查杀，建议使用两款 webshell 查杀工具同时查杀，可相互补充规则库的不足。

六、日志分析

系统日志

分析方法：

a、前提：开启审核策略，若日后系统出现故障、安全事故则可以查看系统的日志文件，排除故障，追查入侵者的信息等。

b、Win+R 打开运行，输入“eventvwr.msc”，回车运行，打开“事件查看器”。

C、导出应用程序日志、安全日志、系统日志，利用 Log Parser 进行分析。

WEB 访问日志

分析方法：

a、找到中间件的 web 日志，打包到本地方便进行分析。

b、推荐工具：

Window 下，推荐用 EmEditor 进行日志分析，支持大文本，搜索效率还不错。

Linux 下，使用 Shell 命令组合查询分析

0x02 工具篇

病毒分析 ：

PCHunter：

http://www.xuetr.com

火绒剑：

https://www.huorong.cn

Process Explorer：

https://docs.microsoft.com/zh-cn/sysinternals/downloads/process-explorer

processshacker：

https://processshacker.sourceforge.io/downloads.php

autoruns：

https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns

OTL：

https://www.bleepingcomputer.com/download/otl/

病毒查杀：

卡巴斯基（推荐理由：绿色版、最新病毒库）：

http://devbuilds.kaspersky-labs.com/devbuilds/KVRT/latest/full/KVRT.exe

大蜘蛛（推荐理由：扫描快、一次下载只能用 1 周，更新病毒库）：

http://free.drweb.ru/download+cureit+free

火绒安全软件：

https://www.huorong.cn

360 杀毒：

http://sd.360.cn/download_center.html

病毒动态：

CVERC-国家计算机病毒应急处理中心：

http://www.cverc.org.cn

微步在线威胁情报社区：

https://x.threatbook.cn

火绒安全论坛：

http://bbs.huorong.cn/forum-59-1.html

爱毒霸社区：

http://bbs.duba.net

腾讯电脑管家：

http://bbs.guanjia.qq.com/forum-2-1.html

在线病毒扫描网站：

多引擎在线病毒扫描网 v1.02，当前支持 41 款杀毒引擎：

http://www.virscan.org

腾讯哈勃分析系统：

https://habo.qq.com

Jotti 恶意软件扫描系统：

https://virusscan.jotti.org

针对计算机病毒、手机病毒、可疑文件等进行检测分析：

http://www.scanvir.com

webshell 查杀：

D 盾_Web 查杀：

http://www.d99net.net/index.asp

河马 webshell 查杀：

http://www.shellpub.com

深信服 Webshell 网站后门检测工具：

http://edr.sangfor.com.cn/backdoor_detection.html

Safe3：

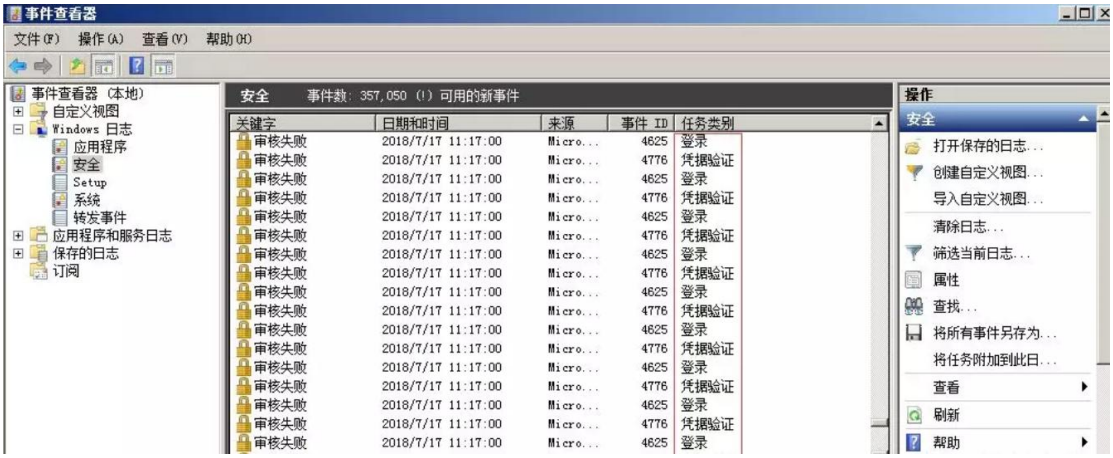
http://www.uusec.com/webshell.zip

0x03 应急响应实战之 FTP 暴力破解

FTP 是一个文件传输协议，用户通过 FTP 可从客户机程序向远程主机上传或下载文件，常用于网站代码维护、日常源码备份等。如果攻击者通过 FTP 匿名访问或者弱口令获取 FTP 权限，可直接上传 webshell，进一步渗透提权，直至控制整个网站服务器。

应急场景

从昨天开始，网站响应速度变得缓慢，网站服务器登录上去非常卡，重启服务器就能保证一段时间的正常访问，网站响应状态时而飞快时而缓慢，多数时间是缓慢的。针对网站服务器异常，系统日志和网站日志，是我们排查处理的重点。查看 Window 安全日志，发现大量的登录失败记录：

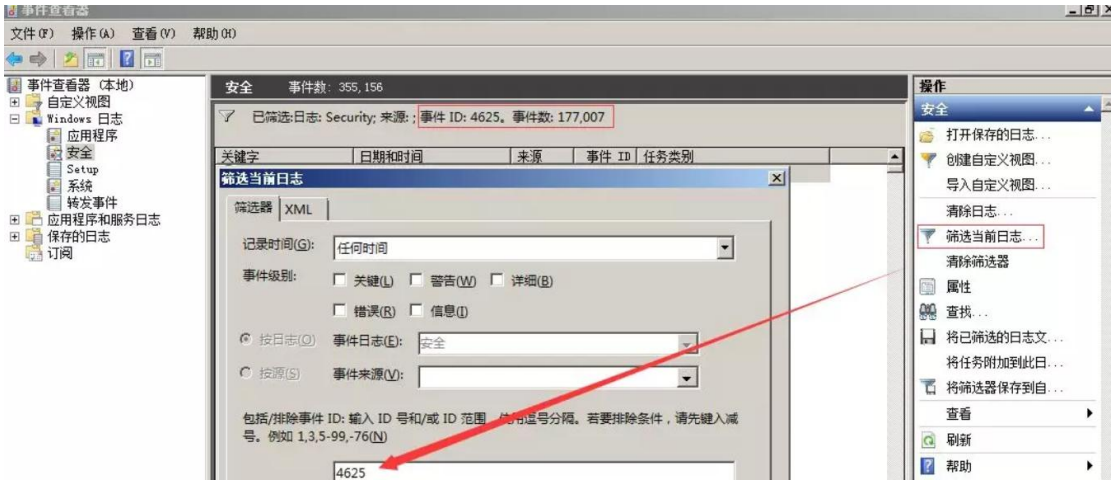


日志分析

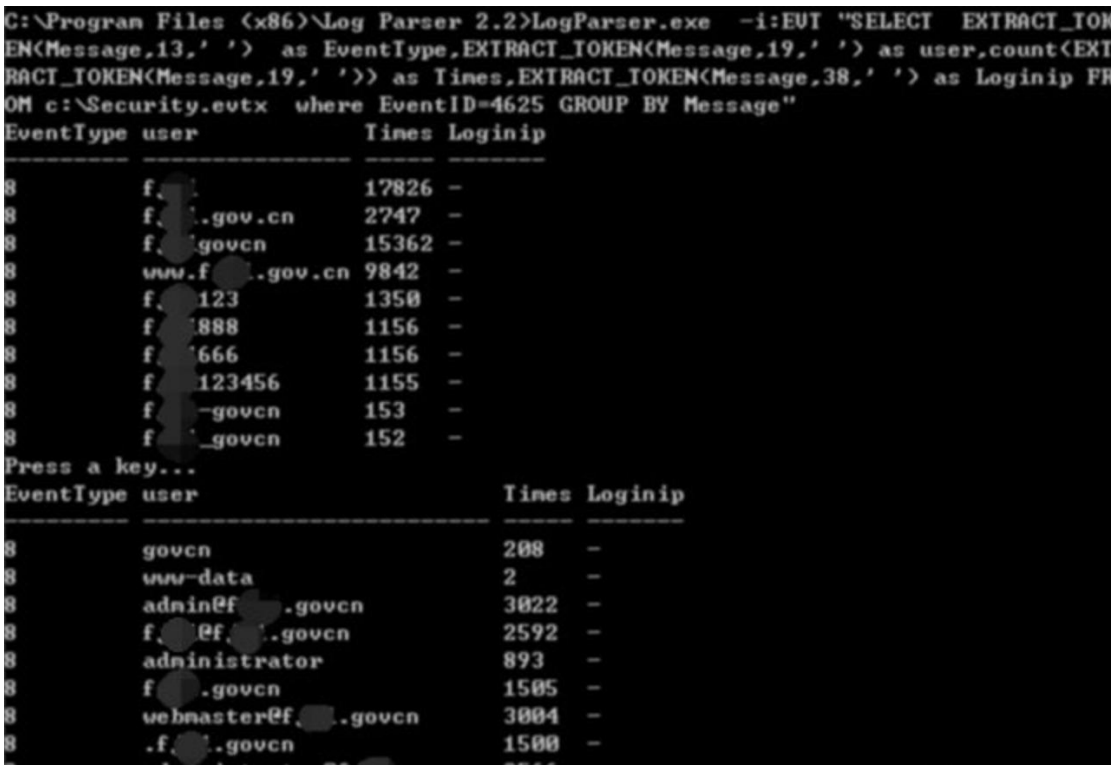
安全日志分析：

安全日志记录着事件审计信息，包括用户验证（登录、远程访问等）和特定用户在认证后对系统做了什么。

打开安全日志，在右边点击筛选当前日志， 在事件 ID 填入 4625，查询到事件 ID4625，事件数 177007，从这个数据可以看出，服务器正则遭受暴力破解：



进一步使用 Log Parser 对日志提取数据分析，发现攻击者使用了大量的用户名进行爆破，例如用户名：fxxx，共计进行了 17826 次口令尝试，攻击者基于“fxxx”这样一个域名信息，构造了一系列的用户名字典进行有针对性进行爆破，如下图：

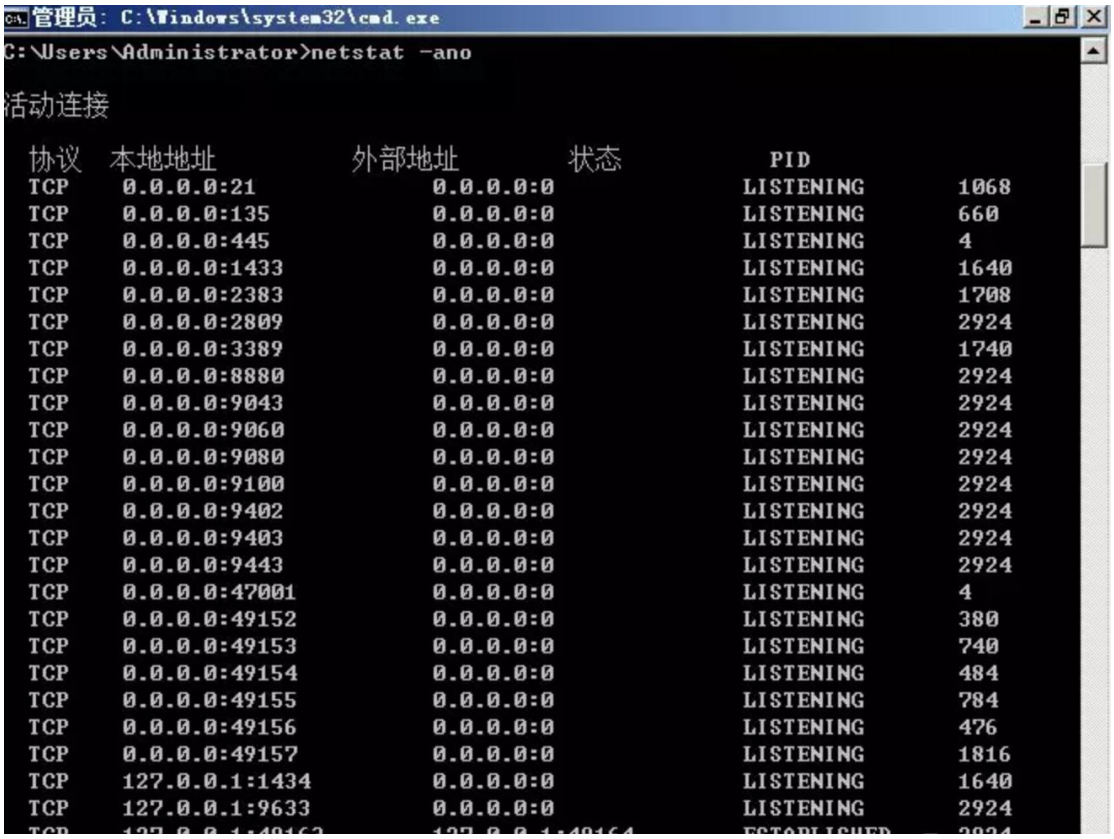


这里我们留意到登录类型为 8，来了解一下登录类型 8 是什么意思呢？

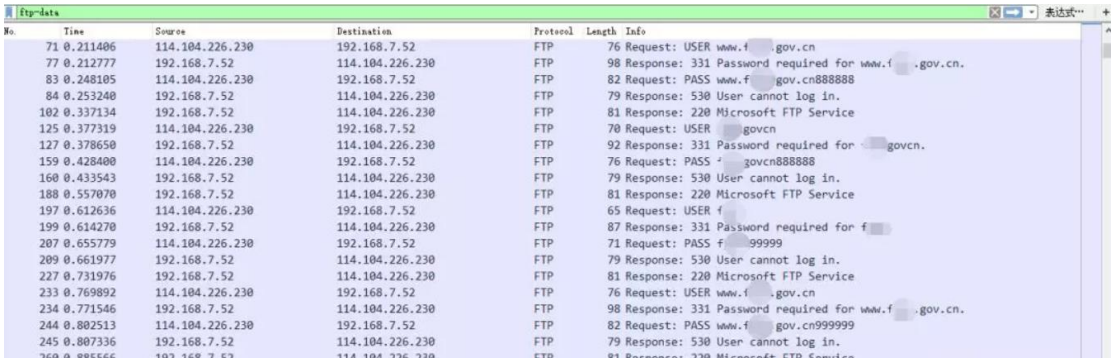
登录类型 8：网络明文（NetworkCleartext）

这种登录表明这是一个像类型 3 一样的网络登录，但是这种登录的密码在网络上是通过明文传输的，WindowsServer 服务是不允许通过明文验证连接到共享文件夹或打印机的，据我所知只有当从一个使用 Advapi 的 ASP 脚本登录或者一个用户使用基本验证方式登录 IIS 才会是这种登录类型。“登录过程”栏都将列出 Advapi。

我们推测可能是 FTP 服务，通过查看端口服务及管理员访谈，确认服务器确实对公网开放了 FTP 服务。



另外，日志并未记录暴力破解的 IP 地址，我们可以使用 Wireshark 对捕获到的流量进行分析，获取到正在进行爆破的 IP：



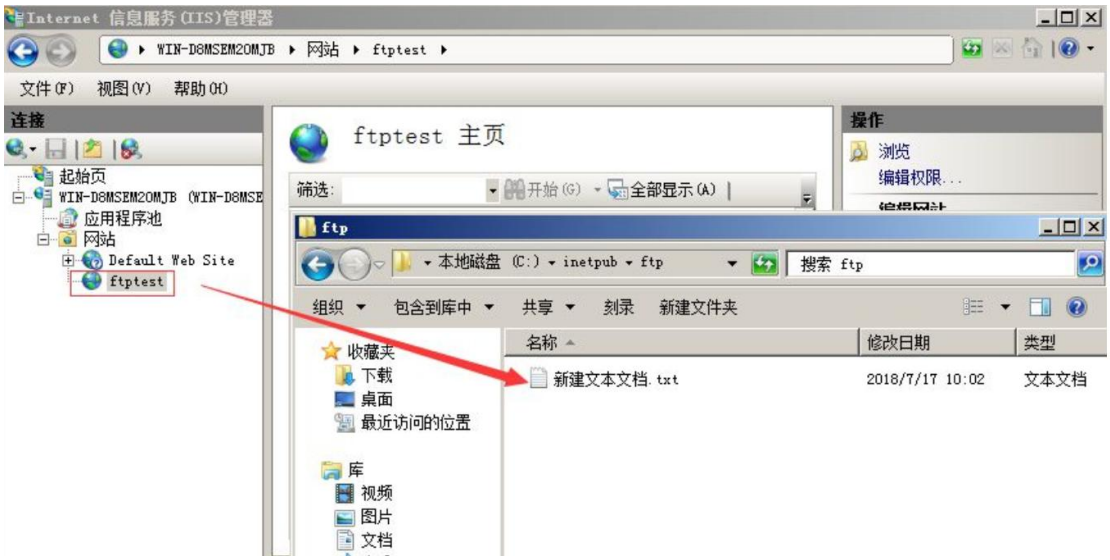
通过对近段时间的管理员登录日志进行分析，如下：

```
C:\Program Files (x86)\Log Parser 2.2>LogParser.exe -i:EVT  "SELECT EXTRACT_TOKE
N(Message,13,' ') as EventType,TimeGenerated as LoginTime,EXTRACT_TOKEN(Strings,
5,'|') as Username,EXTRACT_TOKEN(Message,38,' ') as Loginip FROM c:\Security.evt
x where EventID=4624 and EXTRACT_TOKEN(Message,13,' ')='10'"
EventType LoginTime           Username Loginip
--------- ------------------- -------- -----------
10        2018-07-05 07:26:00  admin 192.168.6.5
10        2018-07-05 07:34:40  admin 192.168.6.5
10        2018-07-05 07:35:07  admin 192.168.6.5
10        2018-07-05 07:48:52  admin 192.168.6.5
10        2018-07-05 08:29:02  admin 192.168.6.5
10        2018-07-05 08:35:21  admin 192.168.6.5
10        2018-07-05 09:55:24  admin 192.168.6.5
10        2018-07-05 10:53:36  admin 192.168.6.5
10        2018-07-05 10:58:20  admin 192.168.6.5
10        2018-07-05 15:07:45  admin 192.168.6.5
Press a key...
EventType LoginTime           Username Loginip
--------- ------------------- -------- -----------
10        2018-07-05 15:18:33  admin 192.168.6.5

Statistics:
-----------
Elements processed: 355852
```

管理员登录正常，并未发现异常登录时间和异常登录 ip，这里的登录类型 10，代表远程管理桌面登录。

另外，通过查看 FTP 站点，发现只有一个测试文件，与站点目录并不在同一个目录下面，进一步验证了 FTP 暴力破解并未成功。



应急处理措施：

1、关闭外网 FTP 端口映射

2、删除本地服务器 FTP 测试

处理措施

FTP 暴力破解依然十分普遍，如何保护服务器不受暴力破解攻击，总结了几种措施：

1、禁止使用 FTP 传输文件，若必须开放应限定管理 IP 地址并加强口令安全审计（口令长度不低于 8 位，由数字、大小写字母、特殊字符等至少两种以上组合构成）。

2、更改服务器 FTP 默认端口。

3、部署入侵检测设备，增强安全防护。

0x04 应急响应实战之蠕虫病毒

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。

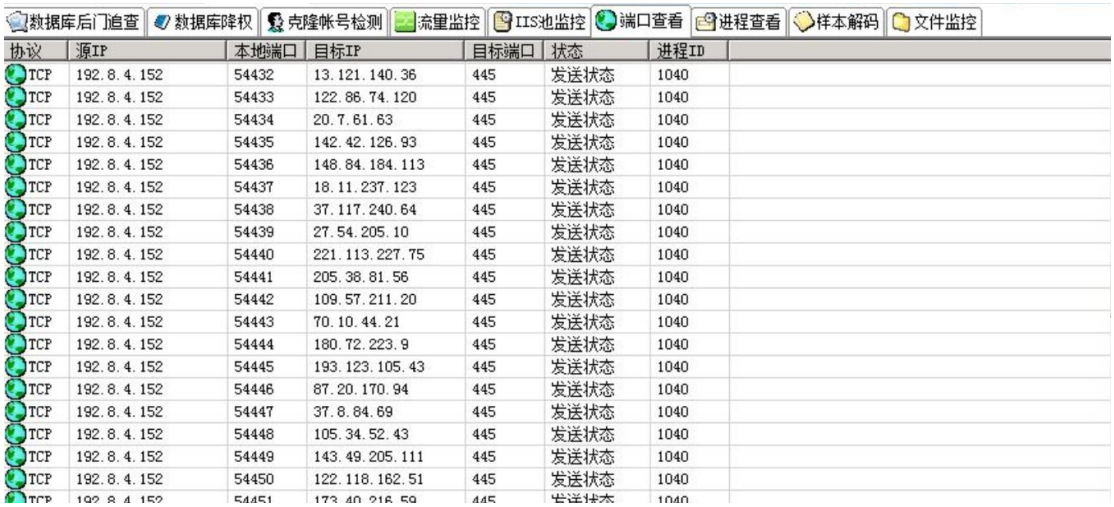
常见的蠕虫病毒：熊猫烧香病毒 、冲击波/震荡波病毒、conficker 病毒等。

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。

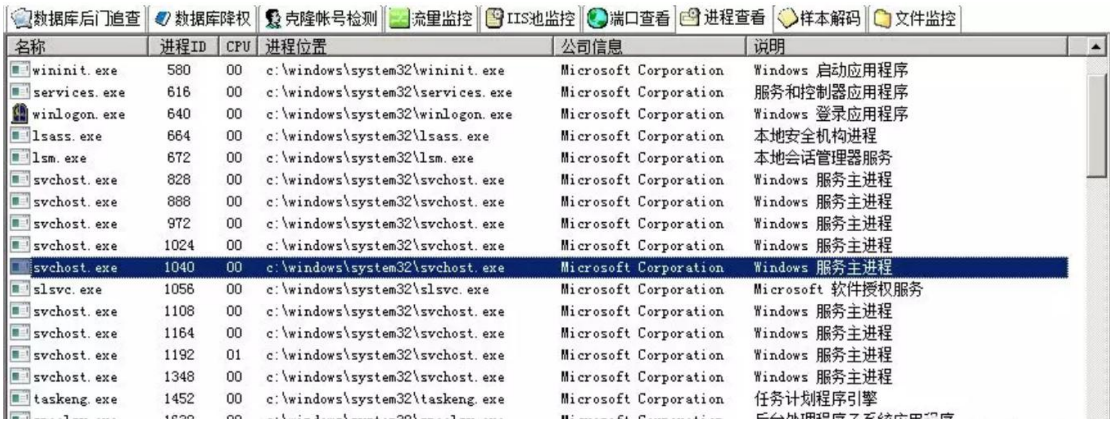
事件分析

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：



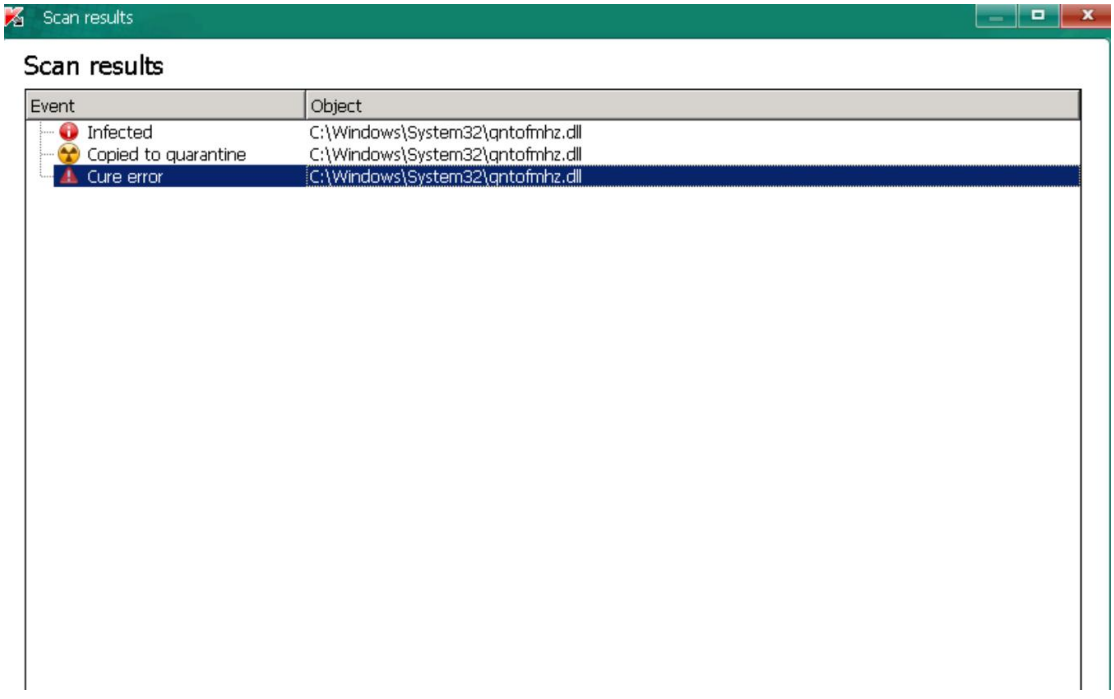
协议	源IP	本地端口	目标IP	目标端口	状态	进程ID
TCP	192.8.4.152	54432	13.121.140.36	445	发送状态	1040
TCP	192.8.4.152	54433	122.86.74.120	445	发送状态	1040
TCP	192.8.4.152	54434	20.7.61.63	445	发送状态	1040
TCP	192.8.4.152	54435	142.42.126.93	445	发送状态	1040
TCP	192.8.4.152	54436	148.84.184.113	445	发送状态	1040
TCP	192.8.4.152	54437	18.11.237.123	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

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

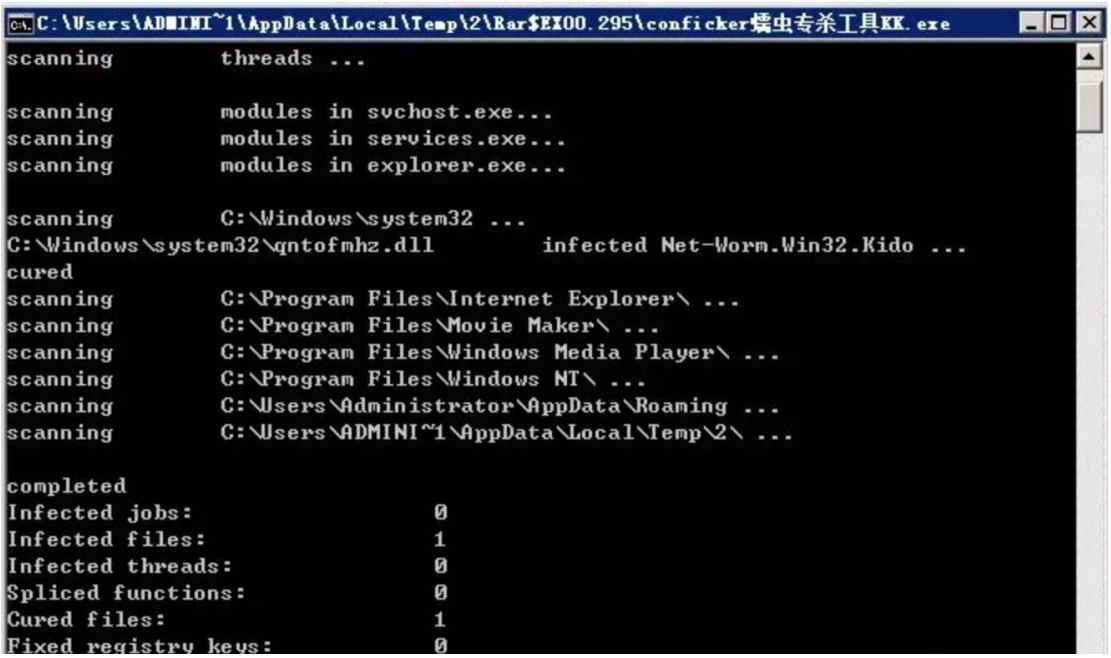
这里我们推测可以系统进程被病毒感染，使用卡巴斯基病毒查杀工具，对全盘文件进行查杀，发现 `c:\windows\system32\qntofmhz.dll` 异常：



使用多引擎在线病毒扫描对该文件进行扫描：

http://www.virscan.org/

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。

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。

0x05 应急响应实战之勒索病毒

勒索病毒，是一种新型电脑病毒，主要以邮件、程序木马、网页挂马的形式进行传播。该病毒性质恶劣、危害极大，一旦感染将给用户带来无法估量的损失。这种病毒利用各种加密算法对文件进行加密，被感染者一般无法解密，必须拿到解密的私钥才有可能破解。自 WannaCry 勒索病毒在全球爆发之后，各种变种及新型勒索病毒层出不穷。

应急场景

某天早上，网站管理员打开 OA 系统，首页访问异常，显示乱码：

事件分析

登录网站服务器进行排查，在站点目录下发现所有的脚本文件及附件都被加密为 .sage 结尾的文件，每个文件夹下都有一个 `!HELP_SOS.hta` 文件，打包了部分样本：

打开 `!HELP_SOS.hta` 文件，显示如下：

到这里，基本可以确认是服务器中了勒索病毒，上传样本到 360 勒索病毒网站进行分析：

http://lesuobingdu.360.cn

确认 web 服务器中了 sage 勒索病毒，目前暂时无法解密。

绝大多数勒索病毒，是无法解密的，一旦被加密，即使支付也不一定能够获得解密密钥。在平时运维中应积极做好备份工作，数据库与源码分离（类似 OA 系统附件资源也很重要，也要备份）。

遇到了，别急，试一试勒索病毒解密工具：

“拒绝勒索软件”网站：

https://www.nomoreransom.org/zh/index.html

360 安全卫士勒索病毒专题：
http://lesuobingdu.360.cn

防范措施

一旦中了勒索病毒，文件会被锁死，没有办法正常访问了，这时候，会给你带来极大的困恼。为了防范这样的事情出现，我们电脑上要先做好一些措施：

1、安装杀毒软件，保持监控开启，定期全盘扫描

2、及时更新 Windows 安全补丁，开启防火墙临时关闭端口，如 445、135、137、138、139、3389 等端口

3、及时更新 web 漏洞补丁，升级 web 组件

4、备份。重要的资料一定要备份，谨防资料丢失

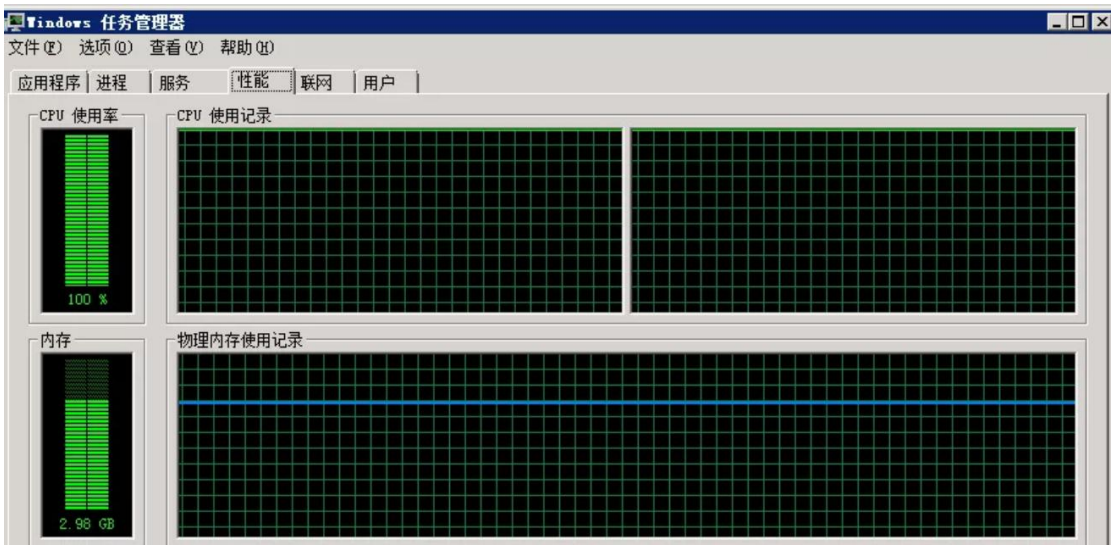
5、强化网络安全意识，陌生链接不点击，陌生文件不要下载，陌生邮件不要打开

0x06 应急响应实战之挖矿病毒

随着虚拟货币的疯狂炒作，挖矿病毒已经成为不法分子利用最为频繁的攻击方式之一。病毒传播者可以利用个人电脑或服务器进行挖矿，具体现象为电脑 CPU 占用率高，C 盘可使用空间骤降，电脑温度升高，风扇噪声增大等问题。

应急场景

某天上午重启服务器的时候，发现程序启动很慢，打开任务管理器，发现 cpu 被占用接近 100%，服务器资源占用严重。

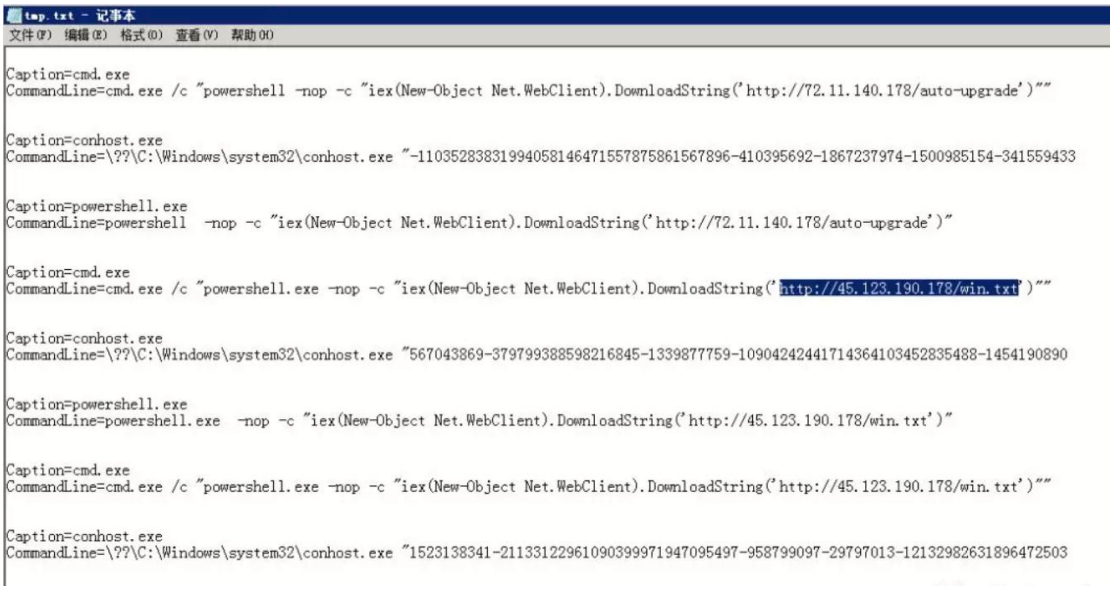


事件分析

登录网站服务器进行排查，发现多个异常进程：

分析进程参数：

wmic process get caption,commandline /value >> tmp.txt



TIPS:

在 windows 下查看某个运行程序（或进程）的命令行参数

使用下面的命令：

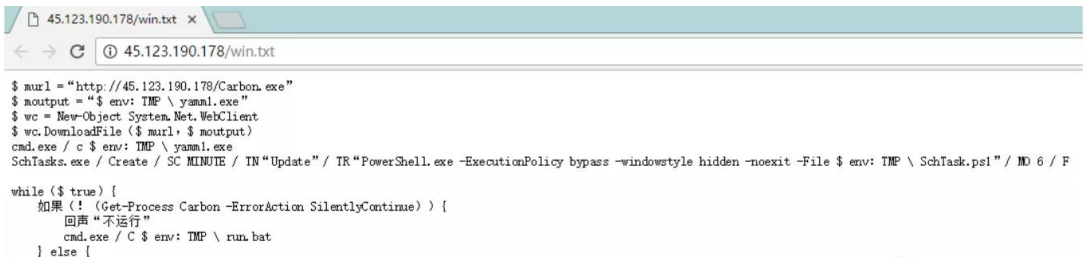
wmic process get caption,commandline /value

如果想查询某一个进程的命令行参数，使用下列方式：

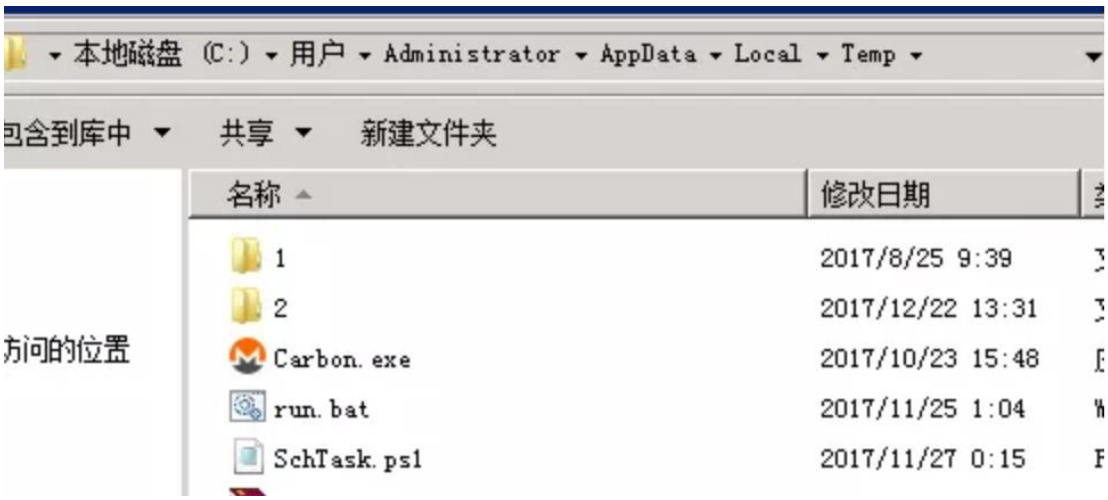
wmic process where caption=”svchost.exe” get caption,commandline /value

这样就可以得到进程的可执行文件位置等信息。

访问该链接：



Temp 目录下发现 Carbon、run.bat 挖矿程序:



具体技术分析细节详见 《利用 WebLogic 漏洞挖矿事件分析》:

https://www.anquanke.com/post/id/92223

清除挖矿病毒：关闭异常进程、删除 c 盘 temp 目录下挖矿程序 。

临时防护方案

1、根据实际环境路径，删除 WebLogic 程序下列 war 包及目录

```
rm -f /home/WebLogic/Oracle/Middleware/wlserver_10.3/server/lib/wls-wsat.war
```

```
rm -f /home/WebLogic/Oracle/Middleware/user_projects/domains/base_domain/servers/AdminServer/tmp/.internal/wls-wsat.war
```

```
rm -rf /home/WebLogic/Oracle/Middleware/user_projects/domains/base_domain/servers/AdminServer/tmp/_WL_internal/wls-wsat
```

2、重启 WebLogic 或系统后，确认以下链接访问是否为 404

http://x.x.x.x:7001/wls-wsat

防范措施

新的挖矿攻击展现出了类似蠕虫的行为，并结合了高级攻击技术，以增加对目标服务器感染的成功率。通过利用永恒之蓝（EternalBlue）、web 攻击多种漏洞，如 Tomcat 弱口令攻击、Weblogic WLS 组件漏洞、Jboss 反序列化漏洞，Struts2 远程命令执行等，导致大量服务器被感染挖矿程序的

现象 。总结了几种预防措施：

1、安装安全软件并升级病毒库，定期全盘扫描，保持实时防护

2、及时更新 Windows 安全补丁，开启防火墙临时关闭端口

3、及时更新 web 漏洞补丁，升级 web 组件