

【应急响应】windows入侵排查思路

作者: Bypass

原文链接: https://mp.weixin.qq.com/s?__biz=MzA3NzE2MjgwMg==&mid=2448903806&idx=1&sn=c7e3cae132ce7469a29fdc170c0a8242&chksm=8b55de23bc2257356ab91be7ef735d26c7340987097fbf8bfae04edb9e1038be306eb5316389&scene=21#wechat_redirect

本文由 干货集中营 收集整理: <http://www.nmd5.com/test/index.php>

0x00 前言

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: 根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，如有管理员组（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。

数据库后门追查
数据库降权
克隆帐号检测
流量监控
IIS池监控
端口查看
进程查看
样本解码
文件监控

ID	帐号	全名	描述	D盾_检测说明
3ED	test\$			危险！克隆了[管理帐号]
3EE	test1\$			带\$帐号（一般用于隐藏帐号）
1F4	Administrator		管理计算机(域)的内置...	[管理帐号]
1F5	Guest		供来宾访问计算机或访...	
3E8	IUSR_WIN2008-NE...	Internet 来宾帐户	用于匿名访问 Interne...	

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 TimeGenerated 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

C:\Program Files <x86>\Log Parser 2.2>
```

微信号: Bypass--

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：

- netstat -ano 查看目前的网络连接，定位可疑的ESTABLISHED
- 根据netstat定位出的pid，再通过tasklist命令进行进程定位 tasklist | findstr "PID"

```
C:\Windows\system32\cmd.exe
C:\Users\Administrator>netstat -ano

活动连接

协议 本地地址 外部地址 状态 PID
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 656
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:1433 0.0.0.0:0 LISTENING 2112
TCP 0.0.0.0:2383 0.0.0.0:0 LISTENING 1352
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING 2608
TCP 0.0.0.0:8080 0.0.0.0:0 LISTENING 2284
TCP 0.0.0.0:47001 0.0.0.0:0 LISTENING 4

C:\Windows\system32\cmd.exe
C:\Users\Administrator>tasklist /f /findstr "2112"
sqlservr.exe 2112 Services 0 97,156 K

C:\Users\Administrator>
```

端口—PID—进程的转换

微信号: Bypass--

2、进程

■ 检查方法:

- 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。
- 打开D盾_web查杀工具，进程查看，关注没有签名信息的进程。
- 通过微软官方提供的 Process Explorer 等工具进行排查。
- 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。

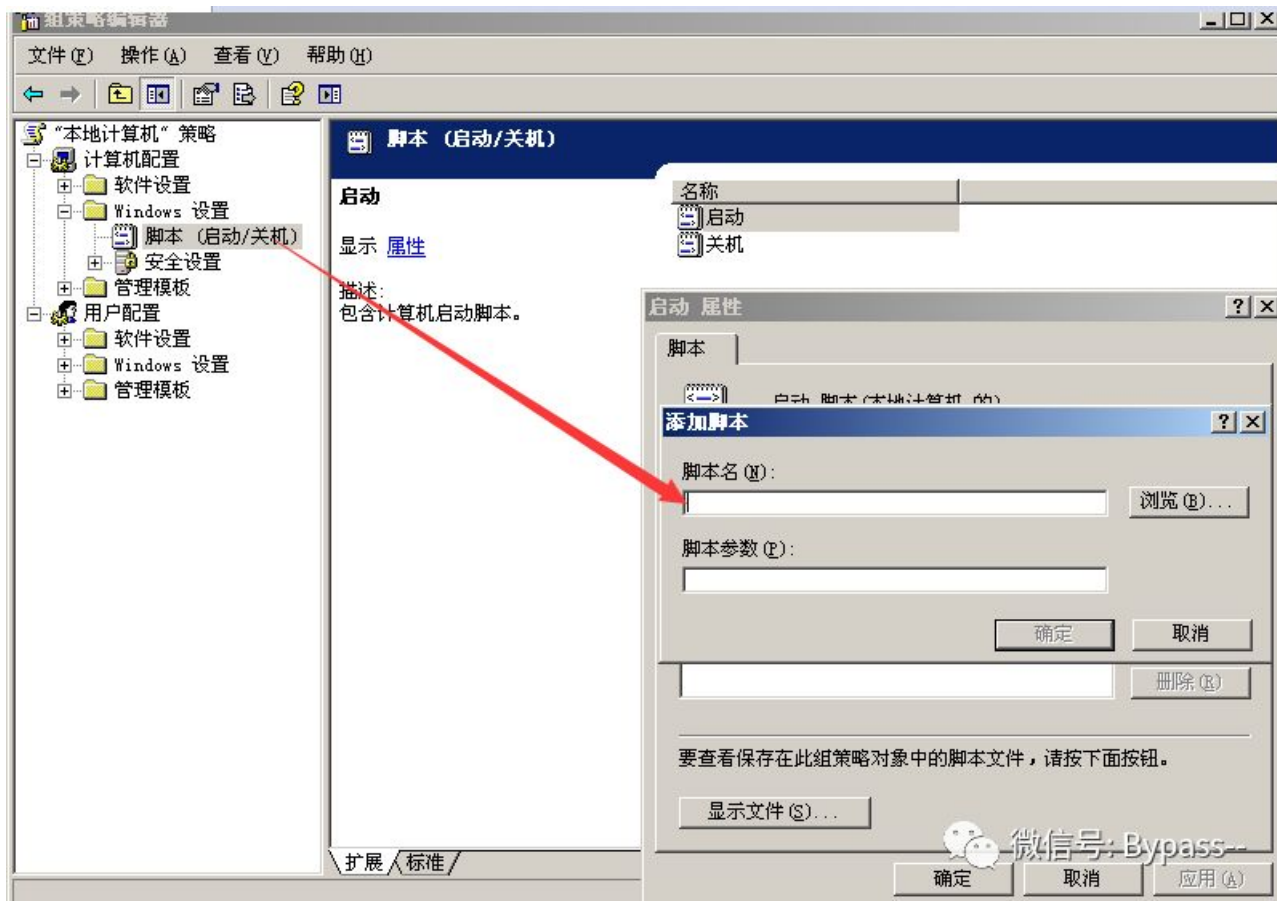
c、单击【开始】>【运行】，输入 regedit，打开注册表，查看开机启动项是否正常，特别注意如下三个注册表项：

```
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

1、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。

2、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

1、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。

2、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

0x03 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  
processhacker: https://processhacker.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: http://devbuilds.kaspersky-labs.com/devbuilds/KVRT/latest/full/KVRT.exe  
(推荐理由: 绿色版、最新病毒库)  
  
大蜘蛛: http://free.drweb.ru/download+cureit+free  
(推荐理由: 扫描快、一次下载只能用1周, 更新病毒库)  
  
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:

<http://www.virscan.org> //多引擎在线病毒扫描网 v1.02, 当前支持 41 款杀毒引擎
<https://habo.qq.com> //腾讯哈勃分析系统
<https://virusscan.jotti.org> //Jotti恶意软件扫描系统
<http://www.scanvir.com> //针对计算机病毒、手机病毒、可疑文件等进行检测分析

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>

本文由Bypass原创发布, 转载请保留出处。欢迎关注我的个人微信公众号: Bypass--, 浏览更多精彩文章。

参考链接:

<https://cloud.tencent.com/document/product/296/9605>

<https://www.cnblogs.com/shellr00t/p/6943796.html>

<https://www.exehack.net/5106.html>

Bypass



About Me

一个网络安全爱好者, 对技术有着偏执狂一样的追求。致力于分享原创高质量干货, 包括但不限于: 渗透测试、WAF绕过、代码审计、安全运维。