【应急响应】 windows 入侵检查流程

应急响应的时候,我们需要判断一个系统是否有被黑客入侵,本篇给大家介绍一些在应急响 应时 Windows 入侵检查的一些知识点。

检查概述

由于无法站在攻击者视角审视其做过哪些攻击行为,因此标准化的检查内容可以规避非标准 化的风险。

例如操作系统虽然没有异常登录日志,但如果不检查操作系统用户即会存在遗漏从而产生风险,同时也可规避上次检查 ab 内容,本次检查 bc 内容的非标准化风险。

因此无论每个人的标准是否统一,取长补短逐渐完善自己的标准化是建议进行的。

windows 操作系统入侵检查流程图如下所示:



现象检查

可通过监测告警、日常巡检等主动机制发现存在的异常事件,如果没有主动发现,则只能在

安全事件发生后被动发现。以卜说明在被入侵后对可能存在的异常现象进行检查。

现象检查发现的异常程序不可直接删除,应先验证异常进程是否存在自我守护机制,否则安 全事件无法得到根除。

1.1 已监听端口

已监听端口并非一个独立的对象,而是和进程相关联,进程如果需要对外提供访问接口,则 必须通过监听端口的方式对外开放,常用于在内网中部署正向后门程序。

注意点:

1 在操作系统初始化正常运行后,建议记录已监听端口的基线值,供日常巡检使用;

2 受操作系统、关键路径中的网络层访问控制影响。

例如检查已监听端口是否存在异常。则运行 cmd 命令行,使用 netstat –ano | findstr LIST 命令检查已监听端口。

示例:

点击【开始菜单】,搜索框中输入【cmd】,右键点击【cmd.exe】程序,选择【以管理员身份运行】。

程序 (1)		
CML cmd. exe	打开 (0) ● 以管理员身份运行 (A) 锁定到任务栏 (K) 附到「开始」菜单 (V) 还原以前的版本 (V)	
	发送到(8) ▶	
	剪切(T) 复制(C)	
	删除 (1)	
	打开文件位置(I)	
	属性(R)	
🔎 查看更多结果		
cmd	区 注销	١



使用 netstat -ano | findstr LIST 命令检查已监听端口。含义如下:

- 1左1列,程序协议;
- 2 左 2 列,本地监听地址和端口;
- 3左3列,外部地址(留空);
- 4 左 4 列, 状态为监听;
- 5 左 5 列,程序 pid。

可根据已知程序不会监听的端口进行判断是否存在异常,并根据该链接的 pid 进行深入分析。

💽 管理员: C: \Tindows\system32\cmd. exe 🖌										
Microsof	t Windows [版本 6.1.760	1]								
版权所有	(c) 2009 Microsoft Cor	poration。保留所有权利。								
C:\Users	\Administrator>netstat	-ano ¦ findstr LIST								
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	0.0.0.0:3306	0.0.0.0:0	LISTENING	248						
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING	1524						
TCP	0.0.0.0:8980	0.0.0.0:0	LISTENING	4						
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING	4						
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING	364						
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING	748						
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	792						
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING	464						
TCP	0.0.0.0:49156	0.0.0.0:0	LISTENING	1560						
TCP	0.0.0.0:49158	0.0.0.0:0	LISTENING	472						
TCP	0.0.0.0:50003	0.0.0.0:0	LISTENING	3956						
TCP	192.168.20.223:139	0.0.0.0:0	LISTENING	4						

1.2 已建立连接

已建立连接分为入站连接和出站连接,入站意为访问操作系统本地的方向,出站意为操作系 统访问外部的方向。

注意点:

1 受操作系统、关键路径中的网络层访问限制影响;

2 服务端如存在主动外联则需要重点检查。

例如检查已建立连接是否存在异常。则使用 netstat –ano | findstr EST 命令检查已建立连接。

示例:

查询结果,可根据非常规连接判断是否存在异常,并根据该链接的 pid 进行深入分析:

管理员: C: \Tindows\system32\cmd. exe		
C:\Users\Administrator>netstat —ano ¦ findstr EST TCP 192.168.20.223:3389 192.168.30.23:60593	ESTABLISHED	1524
C:\Users\Administrator>		

1.3 系统进程

cpu 资源被占满、异常的已监听端口、异常的已建立连接在深入分析时都会检查系统进程。

注意点:不建议使用任务管理器进行系统进程检查,因为可供分析的维度较少,且容易被进 程名欺骗,操作系统允许相同名称但不同执行路径的进程同时存在。

例如检查系统进程是否存在异常,使用以下命令获取系统进程详细信息。

wmic process get

caption,commandline,creationDate,executablepath,handle,handleCount

> c:\yanlian\porcess.txt

示例:

在 cmd 命令行中复制以上命令并回车执行。

打开 C:\yanlian\process.txt, 可看到 6 列内容, 含义如下所示:

1 caption: 进程名;

2 commandline: 进程名、程序执行路径、进程执行参数;

3 creationDate: 进程启动时间(格式为:年月日时分秒);

4 executablepath: 程序执行路径;

5 handle: 进程 pid;

6 handleCount: 该进程的父进程 pid。

可根据进程名、进程执行参数、进程启动时间、程序执行路径判断是否存在异常,并根据异常点进行深入分析。

1 2 3	Caption System Idle Proce System	CommandLine ess		
4 5 7 8 9 10 11 12 13	smss.exe csrss.exe wininit.exe csrss.exe winlogon.exe services.exe lsass.exe lsm.exe svchost.exe svchost.exe	<pre>\SystemRoot\System32\smss.exe %SystemRoot%\system32\csrss.exe wininit.exe %SystemRoot%\system32\csrss.exe winlogon.exe C:\Windows\system32\services.exe C:\Windows\system32\lsass.exe C:\Windows\system32\lsass.exe C:\Windows\system32\lsm.exe C:\Windows\system32\svchost.exe C:\Window</pre>	2 Object 2 Object ke 2 -k Dcc 2 -k RP	tDirector tDirector omLaunch CSS
1 2 3 4 5	CreationDate 20210122142501.632409+480 20210122142501.648009+480 20210122142502.287610+480	ExecutablePath	Handle 0 4 240 312	HandleCount 0 487 35 404

364

376

408

464 472

480

576

656

86

72

214

797

246

356

261

如通过现象检查发现异常程序,则可以通过停止运行该进程的方式,判断其是否会重新启 动。

1.1 任务计划

持久化检查

12

任务计划可以将任何脚本或程序定时启动。如被黑客利用则会充当恶意程序的守护机制。

注意点:不建议使用图形化任务计划程序进行检查,因为数量、层级较多不方便检查。

检查任务计划是否存在异常的方法:

1 使用 schtasks /query /fo LIST /v

>c:\yanlian\schtasks.txt 命令获取任务计划;

2 使用正则 (Folder|TaskName|Status|Author|Task To Run|Scheduled Task State|Start Time|Start Date)(.*) 过滤任务计划关键字段;

20210122142502.490410+480 C:\Windows\system32\wininit.exe

20210122142502.552810+480 C:\Windows\system32\winlogon.exe

20210122142502.740011+480 C:\Windows\system32\services.exe

20210122142503.067611+480 C:\Windows\system32\svchost.exe

20210122142503.239211+480 C:\Windows\system32\svchost.exe

20210122142502.506010+480 C:\Windows\system32\csrss.exe

20210122142502.818011+480 C:\Windows\system32\lsass.exe 20210122142502.818011+480 C:\Windows\system32\lsm.exe 示例 1:

导出任务计划,提示错误。

C:\Users\Administrator>schtasks /query /fo LIST /v > c:\yanlian\schtasks.txt 错误: 无法加载列资源。

C:\Users\Administrator>_

查看当前活动代码页为 936, 将其修改为 437。

C:Wsers Administrator>chcp 活动代码页: 936

C:\Users\Administrator>chcp 437_

再次导出任务计划。但导出的任务计划无关信息过多,需要过滤。

管理员: C:\Windows\system32\cmd.exe

Active code page: 437

C:\Users\Administrator>schtasks /query /fo LIST /v > c:\yanlian\schtasks.txt C:\Users\Administrator>_____

_ 🗆 🗡

示例 2:

复制以下正则表达式。

(Folder|TaskName|Status|Author|Task To

Run|Scheduled Task State|Start Time|Start Date)(.*)

将正则表达式复制到搜索框中,点击【find all】,再【ctrl+c】复制匹配到的内容。

🗾 untitl	ed • - Sublime Text (U	INREGISTE	RED)					_		×
文件(<u>F</u>) 维	扁辑(<u>E)</u> 选择(<u>S</u>) 查找(<u>I)</u> 视图(V)	跳转(<u>G</u>)	<u> 工具(T</u>)	项目(<u>P</u>)	首选项(<u>N</u>)	帮助(<u>H</u>)			
 	untitled	•								▼
1										
2	Folder: \								Billio na nav Di Vilane Di Vilane Di Vilane	
3	HostName:				h	IIN-NE1AJ	P8FADJ		FUF FUF	
4	TaskName:				N	??			IS IN THE A	
5	Next Run Time	:			2	021/2/3	17:18:45			A DESCRIPTION OF THE OWNER OWNER OF THE OWNER
6	Status:				F	leady			BAP BELIER Different BARTIN BART	
7	Logon Mode:				1	interacti	.ve/Backgr	round	DATE AND A	Non Nite Brent Brent Derive
8	Last Run Time	:			N	I/A				
9	Last Result:				1					9-92, Maria
10	Author:				h	IIN-NE1AJ	P8FADJ\Ac	ministr	a	North Contraction
11	Task To Run:				C	:\Window	s\winsxs\	\wow64_m	i.	1000 Lanar

.*	Aa	66 yy	Ċ≡	1	Start Time	Find	Find Prev	Find All	×
	1 of 32	matche	5				Tab Size: 4	Plain Tex	ĸt

同时新建一个文档将复制的内容进行粘贴,但所有任务计划未分割不方便检查,因此还需要 对过滤后的任务计划进行分割。

示例 3:

复制以下正则表达式。

Start Date(.*)

Start Date\$0\n

按【ctrl+h】将以上正则进行粘贴并替换所有。

🗾 Fo	lder: \ • -	Sublime	Text (UN	IREGISTE	RED)						_		\times
文件(<u>F</u>)	编辑(<u>E</u>)	选择(<u>S</u>)	查找(<u>I</u>)	视图(<u>∨</u>)	跳转(<u>G</u>)	<u>工具(T</u>)	项目(<u>P</u>)	首选项(<u>N</u>	<u>Ⅰ</u>) 帮助(<u>H</u>)				
4 •	untitl	ed		Fo	lder: \		•						▼
3	State	is:				Ready						201 House N.J. House and P.P.M. Digital on New York Con- NATIONAL DISTRICT, Name of New York, Name Name of New York, Name of New York, Nam	
4	Auth	or:				WIN-N	E1AJP8FA	DJ\Admin	istrator	C L .		BRUgens over enter d'1911 1807 171 en 1912 1910 - New 1917	
5	Task	IO KUN:	0056-476	1-75 6	1 7600 1	C:\W1		.NSXS\WOW	15 notono	DTT-W1	naow	S - Marco and Arabitation Statements	
6	Sche	huled Ta	sk State	4e55_0.	1.7000.1	Fnahl	e_u50429 ed	74De1104	.13 (nocepac	l.exe		Billion con and Party	
7	Star	t Time:	SK Statt	•		N/A						Billion new Board	
8	Star	t.Date:				•••N/A						SEVERATION CONTRACTOR	
9	Fold	er: \Mic	rosoft									50.76 mm 107*	
10	Fold	er: \Mic	rosoft\W	indows								17 101 17 101	
11	Fold	er: \Mic	rosoft\W	indows\	Active D	irectory	Rights	Manageme	nt Service	es Clie	ent	DT - BIRL	
12	lask	lame:			C1 · + \ AI	\Micr	osoft\Wi	.ndows\Ac	tive Direc	tory	,	SE Burnersen Burnersen Brit	
	Auto	ts manage nated)	ement Se	rvices	Client (Al	U KMS KI	gnts Pol	.icy Temp	late Manag	gement	(125 28 Harr 2076 nor 52 ^m	
.*	Aa "	" Č≡	÷]	Find:	Start Da	te <u>(</u> .* <u>)</u>		•	Find			Replace	×
AB			R	eplace:	Start Da	te\$0\n 🚽	-	▼	Find A	II	F	Replace All	
	1 of 48 ma	tches							Tab	Size: 4		Plain Te	ext

最后形成如下文档:只记录任务计划名称,运行状态,创建者,程序路径,计划状态,启动 时间,以方便对可能存在异常的对象进行检查。

1	Folder: \	
2	TaskName:	/}}
3	Status:	Ready
4	Author:	WIN-NE1AJP8FADJ\Administrator
5	Task To Run:	C:\Windows\winsxs\wow64_microso
	1.7600.16385_none_d5642974be118415\no	tepad.exe
6	Scheduled Task State:	Enabled
7	Start Time:	N/A
8	Start DateStart Date:	N/A
9		
10	Folder: \Microsoft	
11	Folder: \Microsoft\Windows	
12	Folder: \Microsoft\Windows\Active Dire	ectory Rights Management Service
13	TaskName:	<pre>\Microsoft\Windows\Active Dired</pre>
	Client\AD RMS Rights Policy Template #	Management (Automated)
14	Status:	
15	Author:	Microsoft Corporation
16	Task To Run:	COM handler
17	Scheduled Task State:	Disabled
18	Start Time:	3:00:00
19	Start DateStart Date:	2006/11/9

1.2 自启动项

自启动项可在系统启动时自动运行相关程序,恶意程序的第二个自启机制。

注意点:不建议使用图形化 msconfig 工具进行检查,因为名称、路径较长则不方便取证。

使用以下命令将自启动项导出检查。

reg export

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

c:\yanlian\autorun.reg

示例:

输入命令将自启动项配置文件导出。

📷 管理员:C:\Tindows\system32\cmd. exe

C:\Users\Administrator>reg export HKEY_CURRENT_USER\Software\Microsoft\Windows\C_ urrentUersion\Run c:\yanlian\autorun.reg 操作成功完成。

_ 🗆 X

检查导出的自启动项配置是否存在异常。

🧾 autorun. reg - 记事本

文件(F) 编辑(E) 格式(0) 查看(V) 帮助(H)

Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] "notepad"="C:\\Windows\\System32\\notepad.exe"

1.3 环境变量

环境变量用于将系统路径变量化,如被黑客利用则会以最高权限运行恶意程序,例如将环境 变量 %systemroot% 变更为其他路径,同时建立 system32 文件夹并将恶意程序通过服务启 动。

注意点:环境变量 %systemroot% 修改后需进行恢复,否则系统无法正常重启。

使用 set 命令将环境变量导出检查。

示例:

输入命令将环境变量配置文件导出。

管理员: C: \Tindows\system32\cmd. exe	
C:\Users\Administrator>set > c:\yanlian\set.txt	

检查导出的环境变量配置是否存在异常。

4 ►	set.txt ×
31	SystemRoot=C:\Windows
32	TEMP=C:\Users\ADMINI~1\AppData\Local\Temp\2
33	TMP=C:\Users\ADMINI~1\AppData\Local\Temp\2
34	USERDOMAIN=WIN-NE1AJP8FADJ
35	USERNAME=Administrator
36	USERPROFILE=C:\Users\Administrator
37	windir=C:\Windows
38	windows_tracing_flags=3
39	<pre>windows_tracing_logfile=C:\BVTBin\Tests\installpackage\csilogfile.log</pre>
40	

1.4 系统服务

服务可在系统启动时自动运行相关程序或启动后延迟运行相关程序,是恶意程序的第三个自 启机制。 注意点:不建议使用图形化 services.msc 程序进行检查,因为数量、层级较多不方便检查。

1 使用命令将服务配置文件导出检查;

2 过滤包含 Description、ImagePath、ServiceDII 的字段;

3 过滤包含 (.*)(\.dll\.exe)(.*) 的字段;

4 删除 Description REG_SZ, Description

REG_EXPAND_SZ, ImagePath

REG_EXPAND_SZ, ServiceDII

REG_EXPAND_SZ 无关字符

5 将 / Processid(.*) 替换为空;

6 将,-(.*) 替换为空;

7 将 @替换为空;

8 根据环境变量检查结果对 %systemroot%, %windir% 进行替换;

9 将 ^[a-z]*\.dll\n 替换为空;

10 排序、统一小写和去重后进行服务检查。

示例 1:

选择一条命令将服务配置文件导出。

reg query

"HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services" /s > c:\yanlian\service_001.txt

reg query

"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services" /s > c:\yanlian\service_set.txt

🔤 管理员: C: \Windows\system32\cmd. exe

C:\Users\Administrator>reg_guery_"HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Servic

服务配置文件路径说明:

1 ControlSet001:系统真实的服务配置信息;

2 ControlSet002:最后一次成功启动的服务配置信息;

3 CurrentControlSet:系统运行时的服务配置信息;

4 系统启动时,从 ControlSet001 复制到 CurrentControlSet 中;

5 系统运行时,修改的都是 CurrentControlSet 中的信息;

6 系统重启时,从 CurrentControlSet 复制到 ControlSet001 中;

7 系统正常启动时,从 ControlSet001、CurrentControlSet 复制到 ControlSet002;

8 开机选择"最近一次正确配置"时,从 ControlSet002 复制到 CurrentControlSet 中。

服务配置说明:

1 ImagePath:服务所启动程序的路径;

2 Parametes\servicedll: 程序调用的真实 dll 文件路径;

3 Start: 0/boot, 1/system, 2 / 自动, 3 / 手动, 4 / 禁用;

4 DelayedAutostart: 1 / 延迟启动;

5 Type: 程序类型。

示例 2:

输入以下正则表达式进行内容过滤。

(Description|ImagePath|ServiceDII\)(.*)

点击【.*】启用正则匹配,输入正则表达式,点击【find all】后复制。



(.*)(\.dll|\.exe)(.*)

点击【find all】后复制。



示例 4:

复制以下单行内容并逐个替换。

Description REG_SZ

Description REG_EXPAND_SZ

ImagePath REG_EXPAND_SZ

ServiceDII REG_EXPAND_SZ

替换方法为在【find】框中粘贴, 【replace】框中内容为空, 点击【replace all】进行替换。

<	service00		×	ImagePath REG_EXPA	ND_SZ %systemroot	%\system3			▼
2 3 4	2 Description REG_SZ @%SystemRoot%\system32\aelupsvc.dll,-2 3 ServiceDll REG_EXPAND_SZ %SystemRoot%\System32\aelupsvc.dll 4 ImagePath REG_EXPAND_SZ %SystemRoot%\System32\alp.exe								
5	Descr	iptic	on REG_S	Z @%SystemR	oot%\system32	Alg.exe,-113		HALL AND PRODUCTION OF THE SECOND SEC	- U
.*	Aa ""	Ĉ≡	E Find:	Description	REG_SZ	▼	Find	Replace	×
AB			Replace			V	Find All	Replace All]
1	of 139 match	es					Tab Size: 4	Plain Text	

示例 5:

复制以下内容并替换。

/Processid(.*)

替换方法为在【find】框中粘贴, 【replace】框中内容为空, 点击【replace all】进行替换。

4 ►	service001.txt	×	%systemroot%\system32\svchost.exe -k netsvcs	•	•
43	%SystemRoot	%\syste	m32\dllhost.exe 🖊		ingenitering Springer Tradition (1996) 1990/1000 - 1990 - 1990 - 1990 1990/1000 - 1990 - 1990 1990/1000 - 1990 - 1990 1990/1000 - 1990 - 1990
	<pre>Processid:{</pre>	02D4B3F	1-FD88-11D1-960D-00805FC79235}		

.*	Aa	<u>66 99</u>	Ċ≡	÷	Find:	/Processid <u>(</u> .* <u>)</u>	•	Find	Replace	×
AB					Replace:		•	Find All	Replace All	
	1 match	n						Tab Size: 4	Plain Text	

示例 6:

复制以下内容并替换。

,-(.*)

替换方法为在【find】框中粘贴,【replace】框中内容为空,点击【replace all】进行替换。



示例 7:

复制以下内容并替换。

0

替换方法为在【find】框中粘贴, 【replace】框中内容为空, 点击【replace all】进行替换。

<	sei	vice00	1.txt	×	%systemroot%\system32\svchost.exe -k ne	tsvcs •		▼
46	5 🧕	6Syst	temRc	ot%\system	32\cryptsvc.dll		indextriper (grange), y and an and a second se	
.*	Aa	66 yy	Ċ≡	🔠 Find:	@	Find	Replace	×
AB				Replace:	▼	Find All	Replace All	
	18 of 14	0 matc	hes			Tab Size: 4	Plain Text	

示例 8:

复制以下内容并替换。

%systemroot% c:\windows

%windir% c:\windows

替换方法为在【find】框中粘贴, 【replace】框中内容为空, 点击【replace all】进行替换。

4 ►	service00	1.txt	×	%systemroot%\system32\svchos	t.exe -k ne	tsvcs •		▼
46	%Syste	emRoc	ot%\system3	2\cryptsvc.dll				
.*	Aa ""	Ċ≡	🔠 Find:	%systemroot%	▼	Find	Replace	×
AB			Replace	c:\windows	▼	Find All	Replace All	
	U 40 of 323 matches Tab Size: 4 Plain Text							

示例 9:

复制以下内容并替换。

^[a–z]*\.dll\n

替换方法为在【find】框中粘贴, 【replace】框中内容为空, 点击【replace all】进行替换。

< >	serv	vice001	l.txt	:	× c	::windows\system32\svchost.ex	æ -k netsvcs	•		▼
210) <mark>ol</mark>	eres	.dll							
.*	Aa	66 yy	¢≡	÷	Find:	^[a-z]*\.dll\n	•	Find	Replace	×
AB					Replace:	I	•	Find All	Replace All	
	10 of 12 i	matche	es					Tab Size: 4	Plain Text	

示例 10:

对过滤后的程序路径进行排序。

									1					
	行	排序(S) ◀			F9									
	行	非序(区分ナ	大小写)		Ctrl+F9									
	整	理行				>								
	整	理选区				>								
<mark>5</mark> c:\p	Hi	ghlight				>	• - Sublime	Te	ext (UNREG	ISTERE	ED)	—		×
文件(<u>F</u>)	编辑(<u>E</u>)	选择(<u>S</u>)	<u> 查找(l)</u>	视图(⊻)	跳转(<u>G</u>)	I	具(<u>T</u>)项目(<u>I</u>	<u>P)</u>	首选项(<u>N</u>)	帮助((<u>H</u>)			
< >	servio	e001.txt		c:\t	ohpstudy_p	oro\(COM\phpStudy	ySe	erver.exe -SCI	M •				▼
1	c:\	phpstud	ly_pro\	\COM\ph	npStudy	/Se	rver.exe	-	SCM					dinanar (
2	c: w	indows\	Micros	soft.NE	T\Fram	iew	ork64\v2.	.0	.50727\a	ispne	t_sta	ate.exe		
3	C:W	indows\	Micros	soft.NE	ET\Fram	iew	ork64\v2.	.0	.50727\n	iscor	svw.e	exe		
4	c: W	indows\	Micros	soft.NE	ET\Fram	iew	ork\v2.0.	.5	0727\msc	orsv	w.exe	ē		
5	C:W	indolde)	convi	cing\Tr		ne	tallon ov	<u> </u>					CONTRACTOR C	
		THOOM2 /	261 ATC	cru8/11	rusteal	.115	carren .ex	(e					UBUIDERS	

全选所有内容将所有大写字母转换为小写。

	转换大小写(A)	>	首字母大写	1		
	自动换行	>	大写	Ctrl+K, Ctrl+U		
	显示代码自动补全	Ctrl+Space	小写 🚩	Ctrl+K, Ctrl+L		
	行排序(S)	F9	大小写互换			
	行排序(区分大小写)	Ctrl+F9			-	
	整理行	>				
	整理选区	>				
🗾 c:\p	Highlight	>	- Sublime Text	(UNREGISTERED)	- 🗆 ×	
文件(<u>F</u>)	编辑(<u>E</u>) 选择(<u>S</u>) 查找(<u>I</u>) 视	№图(<u>V)</u> 跳转(<u>G)</u>]	[具(T) 项目(P)	首选项(<u>N</u>) 帮助(<u>H</u>)		
文件(<u>F</u>) ◀►	编辑(<u>E</u>) 选择(<u>S</u>) 查找(<u>I</u>) 视 service001.cxt ×	见图(<u>V)</u> 跳转(<u>G)</u>] c∖phpstudy_pro∖	L具(I) 项目(P) .com\phpstudyser	首选项(<u>N</u>) 帮助(<u>H</u>) /er.exe -scm		•
文件(<u>F</u>) ▲► 1	编辑(E) 选择(S) 查找(I) 视 service001.ct x c:\phpstudy_pro\c	N图(V) 跳转(G) コ c\phpstudy_pro\ om\phpstudyse	[具(I) 项目(P) .com\phpstudysen erver.exe。-s	首选项(<u>N</u>) 帮助(<u>H</u>) ver.exe -scm ● SCM		-
文件(E) ▲► 1 2	编辑(E) 选择(S) 查找(I) 初 service00.txt c:\phpstudy_pro\c c:windows\microso	观图(V) 跳转(G) ユ c\phpstudy_pro\ om\phpstudyse ft.net\framew	[具(I) 项目(P) .com\phpstudysen erver.exe -s vork64\v2.0	首选项(<u>N</u>) 帮助(<u>H</u>) ver.exe -scm scm .50727\aspnet_st	tate.exe	•
文件(E) ▲ ► 1 2 3	编辑(E) 选择(S) 查找(I) 视 service001.xt c:\phpstudy_pro\c c:windows\microso c:windows\microso	№图(⊻) 跳转(G) 」 c\phpstudy_pro\ om\phpstudyse ft.net\framew ft.net\framew	具(I) 项目(P) (com\phpstudysen erver.exe -s vork64\v2.0 vork64\v2.0	首选项(<u>N</u>) 帮助(<u>H</u>) /er.exe -scm ・scm ・50727∖aspnet_st ・50727∖mscorsvw・	tate.exe .exe	,
文件(E) ▲ ▶ 1 2 3 4	编辑(E) 选择(S) 查找(I) 视 service00.cd c:\phpstudy_pro\c c:windows\microso c:windows\microso c:windows\microso	N图(Y) 跳转(G) 」 c\phpstudy_pro\ om\phpstudyse ft.net\framew ft.net\framew ft.net\framew	具(I) 项目(P) (com/phpstudysen erver.exe - vork64/v2.0 vork64/v2.0 vork64/v2.0	首选项(№) 帮助(<u>H</u>) ver.exe -scm scm .50727\aspnet_st .50727\mscorsvw. 0727\mscorsvw.ex	tate.exe .exe Ke	-
文件(E) ▲ ▶ 1 2 3 4 5	编辑(E) 选择(S) 查找(I) 视 service00.cxt c:\phpstudy_pro\c c:windows\microso c:windows\microso c:windows\microso c:windows\microso	N图(Y) 跳转(G) エ c\phpstudy_pro\ om\phpstudyse ft.net\framew ft.net\framew ft.net\framew ng\trusteding	具(I) 项目(P) com\phpstudysen erver.exe - s vork64\v2.0 vork64\v2.0 vork(v2.0.56 staller.exe	首选项(<u>N</u>) 帮助(<u>H</u>) ver.exe -scm scm .50727\aspnet_st .50727\mscorsvw.ex	tate.exe .exe ke	

对过滤后的程序路径进行去重。

	整理	11日			>	<u>ن</u> ا	庐	1					
	整理	しまして			>	🔶 🕇	重复	_					
🗾 c:\p	Hig	hlight			>	Fi	刨机打乱	E	GISTERED)		_		×
文件(<u>F</u>)	编辑(<u>E</u>)	选择(<u>S</u>)	查找(<u>l</u>)	视图(⊻)	跳转(<u>G</u>)	工具(<u>T</u>)	项目(<u>P</u>)	首选项	〔(<u>N</u>) 帮助(<u>I</u>	<u>+</u>)			
<	service	2001.txt		c:\t	hpstudy_pr	o\com\p	hpstudyser	ver.exe -	-scm •				▼
1	c:\p	ohpstud	y_pro\	com\ph	pstudys	server	•.exe -	scm				Calculation and a second secon	
2	c:wi	indows\	micros	soft.ne	et\frame	eworke	54\v2.0	.5072	7\aspnet	:_stat	e.exe		- 1
3	c:wi	indows\	micros	soft.ne	et∖frame	eworke	54\v2.0	.5072	7\mscors	w.ex	æ		
4	c:wi	indows\	micros	soft.ne	et\fram∈	work	v2.0.5	0727\	mscorsvw	i.exe		10010074.dasa 100100703044 1001007074 1001007074	
5	c:wi	indows\	servio	cing\tr	ustedir	nstall	ler.exe						
🔲 Li	ne 3, Colui	mn 14							Та	b Size: 4		Plain Tex	xt

根据去重后的结果可直观的对服务所调用的程序进行检查。例如异常的程序路径,程序名称。同时工作量也会大大减少,因为原先需要分析 9062 行,现在只需要分析 145 行即可, 如在 145 行中发现异常则可查看导出的服务配置文件进行深入分析。

4 ►	service001.txt	×	c:\phpstudy_pro\c	com\phpstudyserver.exe -scm	•
9061	HKEY_LOCAL_	MACHIN	IE\SYSTEM\Con ⁻	trolSet001\Service	≘s∖-
9062	EnableD	HCP	REG_DWORD	0x0	
	service001.txt	×	c:\phpstudy_pro\c	om\phpstudyserver.exe -scm	•
144	c:windows\sy	stem32	\wudfsvc.dll		
145	c:windows\sy	swow64	\perfhost.ex	2	

1.5 用户登录

用户登录可在系统启动登录、注销登录时自动运行相关程序,是恶意程序的第四个自启机 制。

注意点:操作系统中有两处配置文件可用于在登录时启动相关程序。

使用命令将用户登录配置文件导出检查。

示例 1:

复制以下命令:

reg query HKEY_CURRENT_USER\Environment

/v UserInitMprLogonScript >

c:\yanlian\userlogin.txt

reg query

"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows

NT\CurrentVersion\Winlogon" /v Userinit >> c:\yanlian\userlogin.txt

在命令行中粘贴将用户登录配置文件导出检查。

🚾 管理员: 命令提示符

C:\Users\Administrator>reg query HKEY_CURRENT_USER\Environment /v UserInitMprLog onScript > c:\yanlian\userlogin.txt

_ 🗆 ×

C:\Users\Administrator>reg_query_"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v_Userinit_>> c:\yanlian\userlogin.txt

C:\Users\Administrator>_

根据导出的登录配置进行检查。



1.6 svchost 及 dll 劫持

svchost.exe 主要作用是将动态链接库(后缀为. dll 的文件) 以服务的方式运行。svchost.exe

对系统的正常运行非常重要,是不能被结束的。通过服务、dll、com 均可动持汪人到程序中 启动。

注意点:

1 在入侵检查方向,更倾向于将 svchost.exe 作为一个单独的持久化检查项目,而非系统服务,因为检查方法完全不同;

2 同时 svchost.exe 不作为常规检查项,一般根据【现象检查】的结果寻找恶意程序。

存在异常监听端口, pid 指向 svchost.exe 程序, 需检查是否存在异常。通过第三方工具 ProcessExplorer (简称 pe) 检查 svchost.exe 程序。

示例:

通过检查已监听端口,发现"异常"监听,pid 指向 800。

🚾 管理员:	命令提示符				_ 🗆 🗙
C:\Users	\Administrator>netstat	-ano ¦ findstr LIST	¦ findstr 49154		
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING	800	
TCP	[::]:49154	[::]:0	LISTENING	800	

打开任务管理器,发现 pid 800 是 svchost.exe 程序,由于该程序的特性,需使用第三方工具 pe 进行检查。

🜉 Tindows 任务管理器	러					_ 🗆 🗵
文件(17) 选项(0) 查看	F(V) 帮助(H)					
应用程序 进程 服	务 性能	联网 用户				
映像名称	PID 🔺	用户名	CPU	内存(描述	<u> </u>
svchost. exe	800	SYSTEM	00	24,068 K	Windows 朋	务主进程

通过 pe 工具可发现 pid 800 是由服务启动,根据启动路径可发现该程序是由正常路径启动,但程序是否被替换未知,启动的服务是 netsvcs(小白杀手,当初虐了我 n 久),该服务下挂 12 个子服务。

🖃 📰 services. exe	464	4,940 K	8,744 K	服务和校制器应用程序
📑 svchost, eze	576	4,472 K	9,712 K	Windows 服务主进程
📷 svchost, eze	656	3,840 K	7,728 K	Windows 服务主进程
svchost. exe	756	9,320 K	12,060 K	Windows 服务主进程
🖃 📷 svchost. eze 🛛 🖊	800 < 0.0	1 32,652 K	35,420 K	Windows 服务主进程
wuauclt.exe	1912	1, 928 K	6,116 K	Windows Update
svchost.exCommand Line	:		12,776 K	Windows 服务主进程
🖃 📰 svchost. ez 🛛 C: \Window	s\system32\svchos	st.exe -k netsvcs	17,620 K	Windows 服务主进程
dwm.exe ^{Path:}			5,800 K	桌面窗口管理器
svchost. ez Services:	s\System32\svchos	st.exe (netsvcs)	14,932 K	Windows 服务主进程
📷 svchost. ez 🛛 Certifica	te Propagation [0	[ertPropSvc]	10,880 K	Windows 服务主进程
📷 spoolsv.ex Group Pol	icy Client [gpsvo	:]	13,516 K	后台处理程序子系统应用程序
📷 <mark>svchost.ex</mark> IP Helper	[iphlpsvc]		9,376 K	Windows 服务主进程
phpStudySe IKE and A	ng Modules [IKEEXT]	6,768 K		
svchost.ez Server []	sktop configurati spmspServer]	on [SessionEnv]	3,000 K	Windows 服务主进程
svchost.ez System Ev	ent Notification	Service [SENS]	10,504 K	Windows 服务主进程

🗖 💼 svchost, ez	Shell Hardware Detec	tion [ShellHWDetection]	8,864 K	Windows 服务主进程
rdpclip	Task Scheduler [Sche	dule]	5, 952 K	RDP Clip 监视程序
svchost. ez	User Profile Service	[ProfSvc]	5,484 R	Windows 服务主进程
📷 sppsvc. exe	Windows Management I:	nstrumentation [Winmgmt] 12,756 K	Microsoft 软件保护平台
		1 700 %		m: 肌含 全进 纽

在 pe 中双击该程序,点击【tcp/ip】,可发现 49154 端口是服务 schedule 监听。

🗾 svchost	svchost.exe:800 (netsvcs) Properties 📃 🗖											
Image	Performan	ice Per	formance Gra	ph	Disk and	Network	ĺ.					
Services	Threads	TCP/IP	Security	Enviror	nment	Strings	Ĺ					
🗆 Resol	Resolve addresses											
P 🚔	Local Add	ress Remo	te Address	State	Servi	ce 📃	I					
TCP	0.0.0.0:49	154 0.0.0	0.0:0	LIS	Schedu	le	L					

点击【services】,可发现 schedule 服务启动的动态链接库绝对路径是

c:\windows\systemc32\schedsvc.dll,从而发现 49154 端口是哪个程序正在监听。

wchost.exe:800	(netsv	wcs) Properties 📃 🗖
Image Perform	nance	Performance Graph Disk and Network
Services Threads	; та	P/IP Security Environment Strings
Services r	egistered	d in this process:
Service	Di	Path
CertPropSvc	Cer	C:\Windows\System32\certprop.dll
gpsvc	Gro	C:\Windows\System32\gpsvc.dll
IKEEXT	IKE	C:\Windows\System32\ikeext.dll
iphlpsvc	IP	C:\Windows\System32\iphlpsvc. dll 🛛 🧹
LanmanServer	Server	: C:\Windows\system32\srvsvc. dll 🛛 🥖
ProfSvc	Vse	C:\Windows\system32\profsvc. dll 🛛 💋
Schedule	Tas	C:\Windows\system32\schedsvc. dl1
SENS	Sys	C:\Windows\System32\sens.dll
SessionEnv	Rem	C:\Windows\system32\sessenv.dl1
	C2 -	C. LTM - Assert Constant and Street and All
ShellHWDetection	5ne	U: \WINDOWS\System32\ShSVCS. dll
ShellHWDetection Winmgmt	Win	C:\Windows\System32\Shsvcs.dl1 C:\Windows\system32\wbem\WMIsvc.dl1

通过点击【view handles】可显示该程序所调用的 clsid。

🂐 Pr -	ocess	Exj	plore	er -	- S y s	int	ern	als:	-	sys
File	Opti	ons	View	Pr	ocess	Fi	nd	DLL	User	s H
	2		E		60	8	X	M	۲	
Proce	55				1/5		(and)	т	(C+vl)	+ MIL
	csrss	.exe			41	ew It		.es	(C (I I	bi bi

如存在启动、点击某个程序后恶意进程重新启动的情况,则可以对 com 劫持进行检查。

🖃 🧺 explorer. e	ze 🚽	1724 (0.02 54,400 K	59,616 K Windows 侵纲	管理器	Microsoft Corpore	tion	
C Everyth	ing. eze	2580	17,192 K	24,932 K Everything		voidtools		
Type	Name 🔶							
ley .	HKLM\SOFTWARE\Ni	crosoft\Window	s\CurrentVersion\Ez	plorer\FolderDescription	s\[2112AB	0A-C86A-4FFE-A368-0D	96E47012E}\Pro	ropertyBag
íe7	HRLM\SOFTRARE\Mi	crosoft\Window	s\CurrentVersion\Ez	plorer\FolderDescription	15\{240018	3A-6185-49FB-A2D8-4A	92A602BA3}\Pro	ropertyBag
ie7	HKLN\SOFTRARE\Ni	crosoft \Window	s\CurrentVersion\Ez	plorer\FolderDescription	hs\{3214FA	B5-9757-4298-BB61-92	9DEAA44FF}\Pro	ropertyBag
.e7	HKLM\SOFTRARE\Ni	crosoft\Window	s\CurrentVersion\Ez	plorer\FolderDescription	15\{33E281	30-4E1E-4676-835A-98	95C3BC3BB}\Pro	ropertyBag
iey	HRLM\SOFTWARE\Ni	crosoft\Window	s\CurrentVersion\Ez	plorer\FolderDescription	\s\{491E92	2F-5643-4AF4-A7EB-4E	k138D8174}\Pro	ropertyBag
iey	HKLM\SOFTWARE\Mi	crosoft \Window	s\CurrentVersion\Ez	plorer\FolderDescription	\s\14BD8D5	71-6D19-48D3-BE97-42	220080E431\Pro	ropertyBag
107	HALA \ SUF I WARE \AL	CIOSOL4 /MINGOR	z\CurrentVersion\Ez	plorer/FolderDescription	152528a	PD-D3F3-48DD-DP0D-28	C2DBR842DJ\FFC	ropertyBag
ley 	@ 注册表编辑器							
ley ley	文件(F) 编辑(E)) 査看(Y) 收録	儀実(A) 帮助(H)					
ley			/0110AR0A=C96A=4	CE-=+269=03F06F47012F1	- 4	45	e and	教権
le7			12112XD0X C00X 41	The ASSO-ODESSECTORES	그 [음	120 J	*# **	(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(
ley			{24001838-6185-45	FF-AZUS-4A39ZADUZBA3}		(and)	EG_52	(創造木成五)
iey			289A9A43-BE44-40	D57-A41B-587A76D7E7F9}	911	Category 1	EG_DWORD	0x0000004 (4)
le7			2A00375E-224C-49	9DE-B8D1-440DF7EF3DDC}	ab	Icon I	EG_EXPAND_SZ	%SystemRoot%\system32\imageres.dll,-1004 🖊
ley			{2B0F765D-C0E9-41	171-908E-08A611B84FF6}	ab	InfoTin J	EG EXPAND SZ	P%SystemBoot%)system32\shell32.dll =12689
iey.			{2C36C0AA-5812-41	687-BFD0-4CD0DFB19B39}	ab	TeaslizedNees 1	C EVPAND C7	9%SurfamBoot%Countin 29(ab.)132 J11 -24594
.97			(3214FAR5-9757-42	298-BB61-9249DF4444FF3		Locarizednane i	LO_LATARD_3L	ewsystemnootwisystemszismerroz. drz, -54504
107 / 07			[33828130-4E1E-46	276-035A-00305C3BC3BB1		Jiane J	EG_52	MusicLibrary
ley ley		10 N	135E20130-4E1E-40	510-033K-20385C3BC3BBJ		ParentFolder I	EG_SZ	{1B3EA5DC-B587-4786-B4EF-BD1DC332AEAE}
(arr			1352401E8-33BE-42	251-BADS-600/CAEDCF9D}	ab	ParsingName J	EG SZ	::{031E4825-7E94-4dc3-E131-E946E44C8DD5}\{2112AE0A-C86A-4ffe-A368-0DE96E4701

ie7 ie7 ie7 ie7 ie7 ie7
 Ab
 Ref_size

 B
 Stream
 REG_DWORD

 Ab
 StreamResource
 REG_EXPAND_SZ

 Ab
 StreamResourceType
 REG_SZ

Music.library-ms 0x000000001 (1) %SystemBoot%\system32\shell32.dll,-2 LIBRARY

通过点击【view dlls】可显示该程序所调用的 dll 文件。

🂐 Pr	ocess Ex	plore	r – Sysi	intern	als:	
File	Options	View	Process	Find	Handl	le V
	🛃 🚍			🖀 🕺	4	۲
Proce	SS Swetom Id	le Pro	View	DLLs (Ctrl+1	jj L

通过排序可直观的看到是否存在 dll 劫持。

💐 Process Explorer - Sysint	ernals: www.sy	sinternals.co	TIN-NE1AJP8P	ADJ\Administrator]							
File Options View Process Fi	File Options View Process Find DLL Users Help										
🛃 🖉 🚍 🖻 🗔 🍕 🚰	メ 🏘 🌚 🗍										
Process	PID C	PU Private B	Working Set De:	scription	Compan;						
🔝 System Idle Process	0 98.	80 K	24 K								
🖃 🔜 System	4 0.	04 112 K	364 K								
Interrupts	n/a 0.	20 K	K Har	dware Interrupts a							
smss. exe	240	556 K	1,208 K Win	idows 会话管理器	Microso						
CSTSS. exe	312	2,260 K	6,004 K Cli	ent Server Runtime	Microso						
wininit. eze	364	1,732 K	5,060 X Win	dows 启动应用程序	Microso						
n services. exe	464	4,888 K	8,720 K 服务	各和控制器应用程序	Microso						
svchost.exe	576	4,468 K	9,700 K Win	idows 服务主进程	Microso						
svchost.exe	656	3,800 K	7,688 X Win	idows 服务主进程	Microso						
📷 svchost. exe	756	9,184 K	12,024 K Win	idows 服务主进程	Microso						
🖃 📷 svchost. exe 🖊	800 < 0.	01 32,596 K	35, 940 K Win	idows 服务主进程	Microso						
	1010	1 000 ₽	C 11C V 000	J	¥:						
Name 🔶 Description		Company Name	Path								
schedsvc.dll 任务计划程序服务	ŕ	Microsoft Corpor	ation C:\Window	rs∖System32∖schedsvc.d	11						
sechost.dll Host for SCM/S	DDL/LSA Look	Microsoft Corpor	ation C:\Window	rs∖System32∖sechost.dl	1						
secur32.dll Security Suppo	rt Provider	Microsoft Corpor	ation C:\Window	rs∖System32∖secur32.dl	1						
Sens.dll 系统事件通知服务	(SENS)	Microsoft Corpor	ation C:\Window	rs∖System32∖Sens.dl1							
Sensapi.dll SENS Connectiv	ity API DLL	Microsoft Corpor	ation C:\Window	rs∖System32∖SensApi.dl	1						
SessEnv.dll 远程桌面配置服务	ŗ	Microsoft Corpor	ation C:\Window	rs\System32\SessEnv.dl)	1						

1.7 帐号检查

操作系统的账户和密码主要用于本地或远程登录。属于黑客持久化后门的一种方式。

注意点:

1恶意账号可能已隐藏,或通过克隆的方式复制管理员账户,需要通过注册表进行检查;

2 作为主管单位对下辖单位进行攻击溯源时,可通过 mimikatz 工具检查是否存在弱口令,所 有口述证据均不可信。

检查账户是否存在异常:方法如下所示:

1调整注册表权限将账户导出检查;

2 使用 net 命令将账户导出检查。

在 cmd 命令行中输入 regedit 打开注册表。



在注册表

【HKEY_LOCAL_MACHINE\SAM\SAM】处右键选择权限,点击【administrators】,勾选 【读取】,并点击确定。

_ 🗆 ×

剑 注册表编辑器		
文件(F) 编辑(E) 查看(V) 收藏	檥夹(A) 帮助0	0
□…1 计算机 ①…1 HKEY_CLASSES_ROOT ①…2 HKEY_CURRENT_USER □…2 HKEY_LOCAL_MACHINE ①…2 BCD0000000 ①…2 HARDWARE □…2 SAM		
SA■ 的权限		×
安全		
Administrators (WIN-NE1	AJF8FADJ\Admin	nistrators)
	添加(0)	删除(R)
Administrators 的权限(P)	 允许	 拒绝
完全控制 读取 特殊权限		
有关特殊权限或高级设置,请单级"。	韩"高	高级(V)
了解访问控制和权限		

复制以下命令。

reg export

HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users c:\yanlian\user.reg

在命令行中粘贴将账户配置文件导出检查。

🚾 管理员: 命令提示符

C:\Users\Administrator>reg export HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Use_ rs c:\yanlian\user.reg 操作成功完成。

根据导出的账户信息进行检查。

+	user.reg ×
139	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names]
140	@=hex(0):
141	
142	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\Administrator]
143	@=hex(1f4):
144	
145	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\Guest]
146	@=hex(1f5):
147	
148	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\WDAGUtilityAccount]
149	@=hex(3e9):
150	
151	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\yjy1]
152	@=hex(3e8):
153	
154	[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\YunWei\$]
155	@=hex(3ee):

记录该路径下的账户名称 16 进制数。

HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names

例如 YunWei\$ 是 3ee。可在以下注册表中检查其 F 值和 V 值

HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000003EE

其中 F 为权限值,如将 administrator 的 F 值复制给 guest,并启用免密码登录,则会形成 克隆账户的隐藏现象,V 为密码值。 [HKEY LOCAL MACHINE\SAM\SAM\Domains\Account\Users\000003EE] 00,da,00,00,00,00,00 "V"=hex:00,00,00,00,bc,00,00,00,02,00,01,00,bc,00,00,00,0e,00,00,00,00,00,00,\ 08,00,00,00,01,00,00,00,d4,00,00,00,04,00,00,00,00,00,00,00,00,d8,00,00,00,14,\ 00,00,00,00,00,00,00,ec,00,00,00,04,00,00,00,00,00,00,00,f0,00,00,00,04,00, 00,00,00,00,00,00,01,00,14,80,9c,00,00,00,ac,00,00,00,14,00,00,00,44,00,00, 00,02,00,30,00,02,00,00,00,02,c0,14,00,44,00,05,01,01,01,00,00,00,00,00,01, 00,00,00,00,02,c0,14,00,ff,07,0f,00,01,01,00,00,00,00,00,05,07,00,00,00,02,\ 00,58,00,03,00,00,00,00,00,24,00,44,00,02,00,01,05,00,00,00,00,00,05,15,00, 00,00,73,90,6a,6c,d9,c3,72,e4,2a,8a,66,68,ee,03,00,00,00,00,18,00,ff,07,0f, 00,01,02,00,00,00,00,00,05,20,00,00,00,20,02,00,00,00,00,14,00,5b,03,02,00, 01,01,00,00,00,00,00,01,00,00,00,00,01,02,00,00,00,00,00,00,05,20,00,00,00,20, 02,00,00,01,02,00,00,00,00,00,05,20,00,00,00,20,02,00,00,59,00,75,00,6e,00,\ 57,00,65,00,69,00,24,00,00,00,01,02,00,00,07,00,00,00,03,00,01,00,03,00,01, 00,15,91,91,86,79,73,2c,5d,17,b6,79,86,20,0e,b6,a5,03,00,01,00,03,00,01,00

示例 2:

复制以下命令。

net user > c:\yanlian\user.txt

net localgroup administrators >> c:\yanlian\user.txt

在 cmd 命令行中粘贴将账户导出,注意 > 意为覆盖写入, >> 意为追加写入。



根据导出的账户信息进行检查。

 1 1 X 2	······································	· x=7	······································		· · · · · · ·	 · · · · · · · · · · · · · · · · · · ·		
	user.txt	×						
1								
2	\\WIN-NE	E1AJP8FADJ	的用尸帐尸					
3								
4								
5	Administ	trator	Gues	t·····		WDAGUti.	lityAccount	-
6	yjyl 🚽							
7	命令成功	完成。						
8								
9	别名	administr	ators					
10	注释	管理员对计	算机/域有不受	逐限制的完	全访问权			
11								
12	成员							
13								
14								
15	Administ	trator						
16	Guest							
17	WDAGUti]	lityAccount						
18	命令成功	完成。						
19								
								_

痕迹检查

1.1 日志

操作系统日志中记录着攻击成功前和攻击后的相关痕迹。

注意点:日志默认记录 20Mb,达到最大值时优先覆盖旧事件,同时网络安全法要求日志至 少保存 6 个月以上。

将安全日志和系统日志导出检查。

示例:

操作系统安全日志和系统日志默认存储路径:

%SystemRoot%\System32\Winevt\Logs\System.evtx

%SystemRoot%\System32\Winevt\Logs\Security.evtx

使用以下命令将日志导出。

管理员: C:\Tindows\system32\cmd. exe	
Microsoft Windows [版本 6.1.7601] 版权所有 <c> 2009 Microsoft Corporation。保留所有权利。</c>	^
C:\Users\Administrator>copy %SystemRoot%\System32\Winevt\Logs\System.evtx c:\ lian\ 已复制 1 个文件。	yan
C:\Users\Administrator>copy %SystemRoot%\System32\Winevt\Logs\Security.evtx c anlian\ 已复制 1 个文件。	: \y

安全日志典型分析方法:大量事件 id 4625 后第一次 4624,则为操作系统密码暴力破解成功。其中源 ip 可能为空,则需要软硬件资产管理系统支持,定位源工作站的名称,即主机名,特定情况下 windows 可通过 ping 主机名携带 – 4 参数返回 ipv4 地址。或通过不对互联网映射操作系统远程桌面管理端口以及使用堡垒机进行管理可规避操作系统密码暴力破解攻击。

系统日志典型分析方法: id 为 7036 是服务启动 / 关闭的系统事件, 在异常时间启动的服务 需要重点检查, 例如 wmi 服务。

1.2 文件落地

恶意程序保存在硬盘的文件系统中,例如后门程序,后门程序属于非授权的远程管理通道, 黑客可通过该通道未授权管理被入侵的主机,以及随后门文件同时生成的其他恶意程序。

注意点:文件落地不单独进行手工检查,一般根据【现象检查】或【持久化检查】的结果在 硬盘中寻找恶意程序,否则工作量会过大及质量较差,常规恶意程序检查建议通过操作系统 杀毒软件进行。

例如在 1999 年 01 月 01 日发现异常程序对其相关处置后,检查当天是否生成其他异常内容。

1 在 %temp% 目录下创建并修改 test.txt 文件的创建时间为 1999 年 01 月 01 日 00 点 00 分 00 秒,修改时间为 1999 年 01 月 02 日 00 点 00 分 00 秒、访问时间为 1999 年 01 月 03 日 00 点 00 分 00 秒;

2 通过 everything 工具进行检查。

示例 1:

16改义件时间 bat 脚本内谷如下所示:

ChangeDate.bat

```
@echo off
```

```
powershell.exe -command "ls'%temp%\test.txt'| foreach-object {$_.CreationTime
='01/01/1999 00:00:00'; $_.LastWriteTime ='01/02/1999 00:00:00'; $_.LastAccessTime
='01/03/1999 00:00:00'}"
```

pause

#CreationTime 创建时间

#LastWriteTime 修改时间

#LastAccessTime 访问时间

修改后各项时间如下所示:

📄 test. txt 🛔	属性	×
常规 安全	详细信息 以前的版本	
	test. txt	
文件类型:	文本文档(.txt)	
打开方式:	2 记事本 更改 (C)	
位置:	C:\Users\Administrator\AppData\Local\Te	mp
大小:	0 字节	
占用空间:	0 字节	
创建时间:	1999年1月1日,0:00:00	
修改时间:	1999年1月2日,0:00:00	
访问时间:	1999年1月3日,0:00:00	

示例 2:

dc:后跟日期,检查创建时间为 1999 年 01 月 01 日,后缀为.txt 的文件。

2	9 dc:1999/1/1 *. txt - Everything										
文	文件(Jr) 编辑(Jc) 视图(V) 搜索(S) 书签(B) 工具(T) 帮助(H)										
dc	dc:1999/1/1 *.txt										
名	3称	路径				大小	创建时间	修改时间	访问时间		
	test. txt	C:\Users\Ad	ninistrator	\AppData\J	Local\Temp\2	0 KB	1999/1/1 0:00	1999/1/2 0:00	1999/1/3 0:00		
				••	-						

🔎 dm:1999/1/2 te*.* - Everything

	文件(37)	编辑(E)	视图(V)	搜索(S)	书登(B)	工具(T)	帮助(H)					
	dm:1999/1/2 te*.*											
	名称	路径	5				大	小	创建时间	修改时间	访问时间	
l	test.	txt C:\l	Jsers\Admi	nistrator	\AppData\	Local\Tem	p\2 0	КB	1999/1/1 0:00	1999/1/2 0:00	1999/1/3 0:00	

da:后跟时间,检查访问时间为 1999 年 01 月 03 日的文件。

<mark>,0</mark> da: 19	9 da:1999/1/3 - Everything										
文件 (F)	编辑(E)	视图(V)	搜索(S)	书签(B)	工具(T)	帮助	(H)				
da:1999/1	da:1999/1/3										
名称	路径	5					大小	创建时间	修改时间	访问时间	
test.	txt C:\l	Jsers\Admi	nistrator	\AppData\	Local\Tem	np\2	O KB	1999/1/1 0:00	1999/1/2 0:00	1999/1/3 0:00	

通过以上案例可知,在入侵取证时 windows 文件的所有时间完全不可信(linux 只是两项时间不可信),因此文件时间仅作为参考依据。

1.3 无文件落地

wmi 全称 windows 管理规范,其提供大量 api 接口供程序调用;同时也是恶意程序无文件落 地的关键所在,黑客将恶意载荷存储于 wmi 中,并通过持久化机制在内存中通过 powershell 直接调用存储于 wmi 中的恶意载荷,从而实现无文件落地。

注意点:

1 可以将 Windows Management Instrumentation 服务关闭,并将其作为一个基线对象定期 检查是否被恶意开启。因为 wbemtest.exe 或 powershell 均是通过该服务调用【wmiclass】 【对象】【属性】中的【值】;

2 当服务关闭时, wbemtest.exe 可打开 wmi 测试器, 但无法连接命名空间, powershell 可 正常运行, 但不会执行 wmiclass 中的载荷;

3 无文件落地不单独进行手工检查,一般根据【现象检查】或【持久化检查】的结果在 wmiclass 中寻找恶意载荷,否则工作量会过大及质量较差,常规恶意程序检查建议通过操作 系统杀毒软件进行。

检查 wmiclass 是否存在异常:

1 搭建无文件落地场景;

2 对无文件落地场景进行检查。

示例 1:

对以下字符串进行 base64 编码:

不能使用网页版 base64 编码工具进行编码,因为编码方式不同会导致 powershell 无法识别,上述命令通过网页版 base64 工具编码后再通过 powershell 识别,其结果如下所示:

瑳牡≁潰敷獲敨汬∠楰柿幺�□�□�□��

因此可通过以下 powershell 工具将其 base64 编码。将命令复制到【\$string】中,当存在【\$】【"】符号时需要使用【`】进行转义,多行内容可直接回车。

ps_string_base64.ps1

\$string = "start powershell `"ping 114.114.114.114 -t`""

\$bytes = [System.Text.Encoding]::Unicode.GetBytes(\$string)

\$encoded = [Convert]::ToBase64String(\$bytes)

echo \$encoded

当前目录下打开 cmd 执行 powershell -executionpolicy bypass -file ps_string_base64.ps1 即可获得 base64 后的字符串。

C:\Windows\System32\cmd.exe -		×
	∖ps ba	se64 ^
转换>powershell -ExecutionPolicy bypass -file ps_string_ba	ise64. p	s1
cwBOAGEAcgBOACAAcABvAHcAZQByAHMAaAB1AGwAbAAgACIAcABpAG4AZw	AgADEA	MQAO
AC4AMQAxADQALgAxADEANAAuADEAMQAOACAALQBOACIA		

打开 poershell 输入以下命令(可以将以下内容 base64 编码化,从 cc 主控端拉取执行,执 行完毕即从内存中释放,这可能也是在被入侵主机中没有发现此类样本的原因),以下命令 通过 powershell 调用. net 的方法将 base64 字符串写入 wmiclass 同时执行。

#要连接的 wmi 命名空间及类对象

\$SaveClass

= [System.Management.ManagementClass]

('root\default:StdRegProv')

#添加对象属性(名称,类型,非数组)

\$SaveClass.Properties.Add('ping',[System.Management.CimType]::String,\$False)

#修改 ping 属性的值为 base64 字符串

\$SaveClass.SetPropertyValue('ping','cwB0AGEAcgB0ACAAcABvAHcAZQByAHMAaABIAGw AbAAgACIAcABpAG4AZwAgADEAMQA0AC4AMQAxADQALgAxADEANAAuADEAMQA0AC

AALQBOACIA')

#保存

\$SaveClass.Put()

#查询 ping 属性的值

\$SaveClass.GetPropertyValue('ping')

#取载荷执行后退出

set ping

([WmiClass]'root\default:StdRegProv').Properties['ping'].Value;powershell -E \$ping;exit

.net 帮助文档参考链接如下所示:

https://docs.microsoft.com/zh-

cn/dotnet/api/system.management.managementbaseobject.setpropertyvalue?

view=dotnet-plat-ext-

5.0#System_Management_ManagementBaseObject_SetPropertyValue_System_String_Syst em_Object_

通过此类方法可发现存储于 wmiclass 中的载荷已被执行,但却不见其父进程,严重影响到溯 源的逻辑性,即无法根据痕迹溯源该程序如何启动,只能通过经验判断可能的自我守护机 制。

如持久化机制未被发现,则无法根除,因此在【现象检查】伊始即强调,在未确认是否存在 自我守护机制前,不可先行删除异常程序。逆向思维考虑:如结束进程后频繁自启动,则一 定存在自我守护机制。

□ 🚔 explorer. exe ⊉ procexp64. exe	1724 0.04 580 0.66	37,612 K 18,032 K	58,992 K Windows 资源管理器 M 29,408 K Sysinternals Process S	Nicrosoft Corporation Sysinternals - www
Dowershell.exe	2020 2352 < 0.01	1,880 K 52,532 K 1,328 K	5,532 K 12 争本 A 48,436 K Windows PowerShell M 3,680 K TCP/IP Ping 命令 M	herosoft Corporation Gierosoft Corporation Gierosoft Corporation
🔁 powershell. exe: 2020 Propert	ties	_ [🗆 🔀 管理员:C: \Tindows\Syst	tem32\WindowsPowerShell\v1.0\powershell.exe
TCP/IP Security Environment .NE' Image Performance Performance Image File Windows PowerShell Microsoft Corporation Version: 6.1.7600.16385 Build Time: Tue Jul 14 07:49:07 20 Path: C:\Windows\System32\WindowsPowerShell\v1.0\pow Command line: !s2\WindowsPowerShell\v1.0\pow Current directory: C:\Users\Administrator\ Autostart Location: n/a Parent: <non-existent process<="" td=""></non-existent>	T Assemblies .NET Pa as Graph Disk and N 109 owerShell\v1.0\powers tershell.exe" ping 114.3 (2616)	rformance Strin etwork Thread hell.c Explore 14.114.114 -t Explore	来自114.114.114.114 東自114.114.114.114 東京自114.114.114.114 東京自114.114.114.114 <td< td=""><td>的回复:字节=32 时间=12ms TTL=86 的回复:字节=32 时间=12ms TTL=66 的回复:字节=32 时间=12ms TTL=64 的回复:字节=32 时间=12ms TTL=94 的回复:字节节=32 时间=12ms TTL=94 的回复:字节节=32 时间=12ms TTL=94 的回复:字节节=32 时间=12ms TTL=94 的回复:字节节=32 时间=12ms TTL=94 的回复:字节节=32 时间=12ms TTL=94 的回复复:字节节=32 时间=12ms TTL=93 的回复复:字节节=32 时间=12ms TTL=99 的回复复:字节节=32 时间=12ms TTL=99 的回复复:字节节=32 时间=12ms TTL=99 的回复复:字节节=32 时间=12ms TTL=98 的回复复:字节节=32 时间=12ms TTL=93 的回复复:字节节=32 时间=12ms TTL=88 的回复复:字节节=32 时间=12ms TTL=88 的回复复:字节节=32 时间=12ms TTL=88 的回复复:字节节=32 时间=12ms TTL=89 的回复复:字节节=32 时间=12ms TTL=88</td></td<>	的回复:字节=32 时间=12ms TTL=86 的回复:字节=32 时间=12ms TTL=66 的回复:字节=32 时间=12ms TTL=64 的回复:字节=32 时间=12ms TTL=94 的回复:字节节=32 时间=12ms TTL=94 的回复:字节节=32 时间=12ms TTL=94 的回复:字节节=32 时间=12ms TTL=94 的回复:字节节=32 时间=12ms TTL=94 的回复:字节节=32 时间=12ms TTL=94 的回复复:字节节=32 时间=12ms TTL=93 的回复复:字节节=32 时间=12ms TTL=99 的回复复:字节节=32 时间=12ms TTL=99 的回复复:字节节=32 时间=12ms TTL=99 的回复复:字节节=32 时间=12ms TTL=98 的回复复:字节节=32 时间=12ms TTL=93 的回复复:字节节=32 时间=12ms TTL=88 的回复复:字节节=32 时间=12ms TTL=88 的回复复:字节节=32 时间=12ms TTL=88 的回复复:字节节=32 时间=12ms TTL=89 的回复复:字节节=32 时间=12ms TTL=88

以下命令可在前台运行时将载荷带入后台运行,诸如任务计划运行的程序默认在后台运行:

start powershell -NoP -Nonl -W Hidden "ping 114.114.114.114 -t"

示例 2:

根据 pe 检查结果无法判断该进程的父进程,即无法确认该进程如何启动,仔细检查任务计划 时发现异常:

🕑 任务计划程序	
文件()) 操作(A) 查看(V) 帮助(H)	
🗢 🔿 🚈 💽 🔽 🗊	
④ 任务计划程序(本地)	名称 状态 触发器
□ □● 11分け別程序库 〒 □● Microsoft	est 准 在 2021/2/8 的 13:02 时
🔮 test 属性(本地计算机)	×
「常规」「触发器」操作」」条件」「设置」「历史记录(已	(禁用) Ì
团建社务时,可以指定服友该社务的条件。	
一次 在 2021/2/8 的 13:02 时 - 触发后 , 无限期	肺每隔1小时重复一次。 已启用

e	test 属性(4	地计算机	ቢ)	x
	常规 触发器	暑 操作	条件 设置 历史记录(已禁用)	
	创建任冬时	心须指完	4. 经合款时发生的操作。	
	CONFLEXANT /	2077347		
	操作		详细信息	
	启动程序		C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -E	
	put_ va iclas	ss. ps1 –	- 记事本	
文	件(牙) 编辑(3	() 格式((0) 查看(V) 帮助(H)	
-E	; BIAU∩ATAB	«ለርኩልኩ»	-Brod Code A Road to Brod the A Road De La Cada a Brod Code a A Road A Roa	-ACOAZOB
mA	GEAdQBsAH	QAOgBz <i>i</i>	AHQAZABYAGUAZwBwAHI AbwB2ACcAKQAuAFAAcgBvAHAAZQByAHG	QAaQB1AH
MA	WwAnAHAAa(QBuAGel	AJwBdAC4AVgBhAGwAdQB1ADsAcABvAHcAZQByAHMAaAB1AGwAb/	AgACOAR
Non	ISHCAHCHDD	AG4ALWI	ктаболедоралыд	
在角	解码时不建	议使用	网页版 base64 解码工具,因为大部分网页工具默认会按:	多字节解码,
₽¥	数每个字符	后会再	补一个字节内容,如下所示:	



cwBIAHQAIABwAGkAbgBnACAAKABbAFcAbQBpAEMAbABhAHMAcwBdACcAcgBvAG 8AdABcAGQAZQBmAGEAdQBsAHQAOgBzAHQAZAByAGUAZwBwAHIAbwB2ACcAKQ AuAFAAcgBvAHAAZQByAHQAaQBIAHMAWwAnAHAAaQBuAGcAJwBdAC4AVgBhAG wAdQBIADsaCABvAHcAZQByAHMAaABIAGwAbAAgAC0ARQAgACQAcABpAG4AZwA 7AGUAeABpAHQA

因此可通过以下 powershell 工具将其 base64 解码。将 base64 字符串复制到【\$string】 中, GetString() 方法建议使用 Unicode, 如改成 utf8, 则会在每个字符后面补一个空格。

ps_base64_string.ps1

\$string =

"cwBIAHQAIABwAGkAbgBnACAAKABbAFcAbQBpAEMAbABhAHMAcwBdACcAcgBvAG8Ad ABcAGQAZQBmAGEAdQBsAHQAOgBzAHQAZAByAGUAZwBwAHIAbwB2ACcAKQAuAFAA cgBvAHAAZQByAHQAaQBIAHMAWwAnAHAAaQBuAGcAJwBdAC4AVgBhAGwAdQBIADsAc ABvAHcAZQByAHMAaABIAGwAbAAgAC0ARQAgACQAcABpAG4AZwA7AGUAeABpAHQA"

\$bytes =

[System.Convert]::FromBase64String(\$string);

\$decoded =

[System.Text.Encoding]::Unicode.GetString(\$bytes);

当前目录下打开 cmd 执行 powershell -executionpolicy bypass -file ps_base64_string.ps1 即可发现解码后的内容。

检查 wmi 服务,发现其已被未授权启动(默认为自动启动,建议关闭后建立基线值作为日常 自动化巡检的对象)。

Tindows Sanage	ent Instrumentation 的属性(本地计算机)	×
常规 登录	恢复 依存关系	
服务名称:	Winnert	
显示名称:	Windows Management Instrumentation	
描述:	提供共同的界面和对象模式以便访问有关操作 🔺 系统、设备、应用程序和服务的管理信息。如 🛃	
可执行文件的路 C:\Windows\sys	径: tem32\svchost.exe -k netsvcs	
启动类型(B):	自动	
帮助我配置服务	<u>启动洗项。</u>	
服务状态:	已启动	
启动(S)	停止(T) 暂停(P) 恢复(R)	
当从此处启动服	务时,您可指定所适用的启动参数。	
启动参数(91):		
	确定 取消 应用 (A)	

需判断 root\default 命名空间的 stdregprov 类对象的 ping 值是否存在异常。可打开 powershell 通过以下命令进行检查。

\$SaveClass

= [System.Management.ManagementClass]

('root\default:StdRegProv')

\$SaveClass.GetPropertyValue('ping')'

检查结果如下所示:



也可以打开 wbemtest.exe 工具进行检查。

<mark>] 管理员: C:\Tindows\system32\cmd.exe</mark> Microsoft Windows [版本 6.1.7601] 版权所有 <c> 2009 Microsoft Corporation。保留所有权利。 C:\Users\Administrator>wbemtest.exe

点击【连接】。

Tindows Banage	ment Instrumentation 👷	试器 📃 🗵 🗵
命名空间:		
		退出
-IWbemServices-		
おおんみ (17)	始光京師(1) 打工会な	2方向の1 偏線と下文の1

根据残留痕迹,输入【root\default】并点击【连接】。

连接	
命名空间	连接
root\default	取消

点击【枚举类】。

Tindows Management Instrumentation 测试器 📃 🗖 🗙						
命名空间:						
root\default						
_IWbemServices—						
枚举类 (E)	枚挙实例(L)	打开命名空间(1)	编辑上下文(E)			
创建类 (C)	创建实例(B)	查询(Q)	创建刷新器(A)			
打开类 (0)	打开实例 (2)	通知查询(U)				
删除类 @)	删除实例 (L)	执行方法(2)				

勾选【递归】并【确定】	0
-------------	---

超类信息	
输入把米包称	确定
制八連吳有称	取消
○ 且馬 ● 递归	

查询结果	
顶级类	关闭
65 个对象 此处理最大值: 1C 完毕	
Trustee SecurityRelatedClass) Win32Provider _Provider) ActiveScriptEventConsumer _EventConsumer) CommandLineEventConsumer _EventConsumer) LogFileEventConsumer _EventConsumer) NTEventLogEventConsumer _EventConsumer) RegistryEvent ExtrinsicEvent) RegistryEvent _ExtrinsicEvent) RegistryTreeChangeEvent (RegistryEvent) RegistryValueChangeEvent (RegistryEvent) SMTPEventConsumer _EventConsumer) SMTPEventConsumer EventConsumer) SMTPEventConsumer EventConsumer)	

在【属性】中找到 ping 属性,双击编辑属性

StdRegProv 的对象	自相器			
限定符				关闭(C)
dynamic	CIM_BOOLEAN	TRUE		
provider	CIM_SINIS2 CIM_STRING	RegProv		1年1月2月第16月
•		-	•	显示 MOF
添加限定符	编辑限定符	删除限定符		超类
属性	□ 隐藏系统属	<u>────</u> ──	本地	导出
	CIM_SINT32 CIM_STRING	2 (Ox2) StdRegProv	_	
SIPERCLASS	CIM_STRING CIM_STRING	WIN-NE1AJP8FADJ		
calc	CIM_STRING	c:\windows\syste	m32\c:	刷新对象
ping	CIM_STRING	ewBOAGEAcgBOACAA	cABvAl 🚽	
			•	- 更新类型
添加属性	编辑属性	删除属性		○ 只创建
				○ 只更新
CheckAccess				 三者之一
CreateKey				$\sim + \infty$
DeleteValue				● 兼合 ◎ エ ^
EnumKey			-	
•			•	○ 强制
	1			
唐性编辑器				
居耕方均		17 J.		/0 大 民 4

ping	StdRegProv	取消
类型		
CIM_STRING	🗾 🗔 数组	
数值 C NULL	⊙ 非 NULL	
cwBOAGEAcgBOACAAcABv	AHcAZQByAHMAaABlAGwAbAAgACIAcABpA	G4AZ



最终对其进行解码,发现其功能和异常现象一致。

start powershell "ping 114.114.114.114 -t"

\ps base64转换>.\ps_base64_string.ps1

1.4 操作系统防火墙

windows 操作防火墙配置着允许 / 拒绝通行的入站 / 出站规则。可根据防火墙配置判断该主机在同网段内的可攻击面积。

注意点:检查配置前应先检查防火墙是否已启用。

检查操作系统防火墙是否存在异常:

1 通过 netsh 命令将防火墙状态导出检查;

2 通过 netsh 命令将防火墙所有入站、出站规则导出检查;

示例 1:

复制以下命令在 cmd 中执行。

netsh firewall show state > c:\yanlian\firewall-state.txt

netsh advfirewall firewall show rule name=all dir=in > c:\yanlian\firewall-in.txt

netsh advfirewall firewall show rule name=all dir=out > c:\yanlian\firewall-out.txt

【操作模式】为【禁用】意为防火墙已关闭,即已监听的端口同网段所有主机均可访问。

+	firewall-state.txt ×	
1	防火墙状态:	
2		
3	配置文件	= 标准
4	操作模式	= 禁用 🧖
5	例外模式	= 启用
6	多播/广播响应模式	= 启用
7	通知模式	= 启用
8	组策略版本	= Windows 防火墙
9	远程管理模式	= 禁用
10		
11	所有网络接口上的端口当前均为打开状态	5:
12	端口 协议 版本 程序	
13		
14	当前没有在所有网络接口上打开的端口。	

【操作模式】的启用和禁用随网卡的网络位置变更而变更。

例如网卡的网络位置是【家庭网络】或【工作网络】,则匹配家庭或工作(专用)网络位置防 火墙的状态。或网卡的网络位置是【公用网络】,则匹配公用网络位置防火墙的状态。





复制以下正则进行搜索和结果复制:

(已启用丨	本地端口	操作)(.*)
-------	------	---------



即可对入站、出站规则进行检查分析,且工作量也会大大减少。

1297	规则名称:	远程桌面 - RemoteFX (TCP-In)
1298		
1299	已启用:	是
1300	方向:	入
1301	配置文件:	域,专用,公用
1302	分组:	远程桌面 - RemoteFX
1303	本地 IP:	任何
1304	远程 IP:	任何
1305	协议:	тср
1306	本地端口:	3389
1307	远程端口:	任何
1308	边缘遍历:	否
1309	操作:	允许
1310	确定。	
1311		
351	已启用:	是
350	大地端口・	3380
552		5585 -4. ⁵ F
353	探作 :	元计
354		
355	已启用:	是一
356	本地端口:	3389
357	·····································	金许
557	3木 ト・	
358		

windows 终端入站规则应根据实际工作需要进行网络层访问控制,windows 服务端出站规则 应根据实际工作需要进行网络层访问控制。

1.5 操作系统杀毒软件

杀毒软件可用于防护恶意程序的存储、运行等恶意行为,作为主管单位对下辖单位进行攻击 溯源时需进行检查。

注意点:

1 应检查杀毒软件的安装时间;

2 应检查杀毒软件的补丁更新情况;

3 应检查杀毒软件的特征库是否最新;

4 应检查杀毒软件最近的杀毒记录;

应检查杀毒软件的白名单。