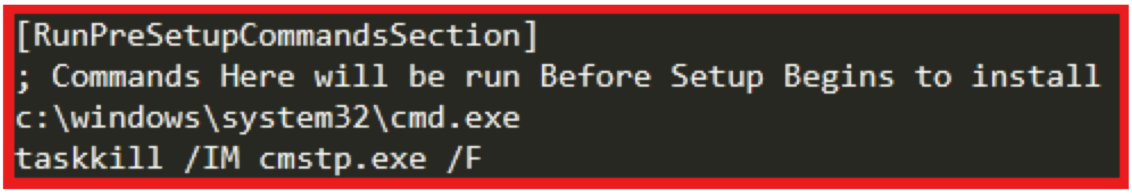
T1191
Connection Manager Profile Installer (CMSTP.exe) 用于安装连接管理服务配置文件，cmstp.exe 可以把 inf 文件做参数来安装一个服务来建立远程网络访问。
cmstp 有三种恶意利用的方式：

１.可以加载执行远程或者本地的 dll 或者 COM scriptlets (SCT)，这个过程可以绕过 AppLocker。
cmstp.exe /s #{inf_file_path}

```
[UnRegisterOCXSection]
%11%\scrobj.dll,NI,C:\Sysmon\T1191.sct
```

https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1191/T1191.inf
https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1191/T1191.sct

２. 通过 inf 文件中的 RunPreSetupCommandSection 来 bypass UAC
cmstp.exe /s #{inf_file_uac} /au

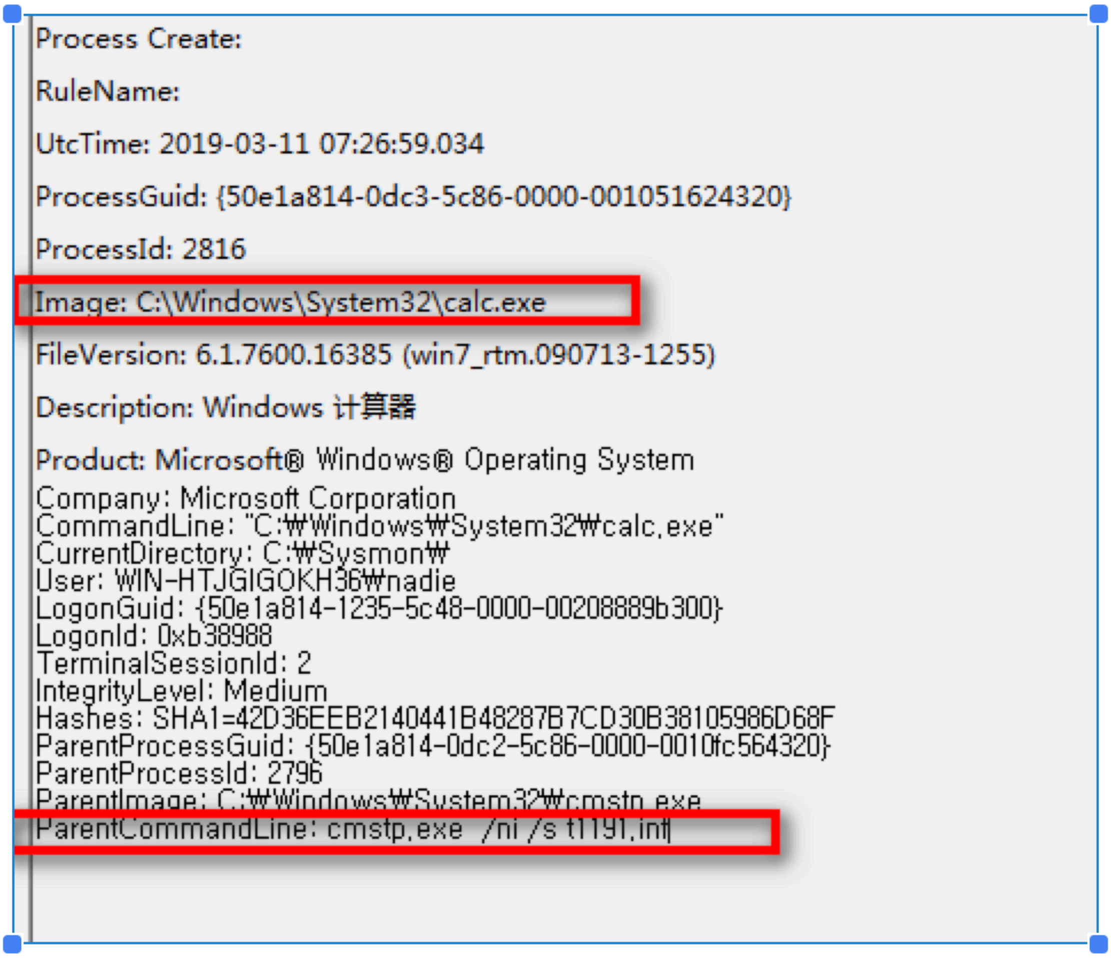


```
[RunPreSetupCommandsSection]
; Commands Here will be run Before Setup Begins to install
c:\windows\system32\cmd.exe
taskkill /IM cmstp.exe /F
```

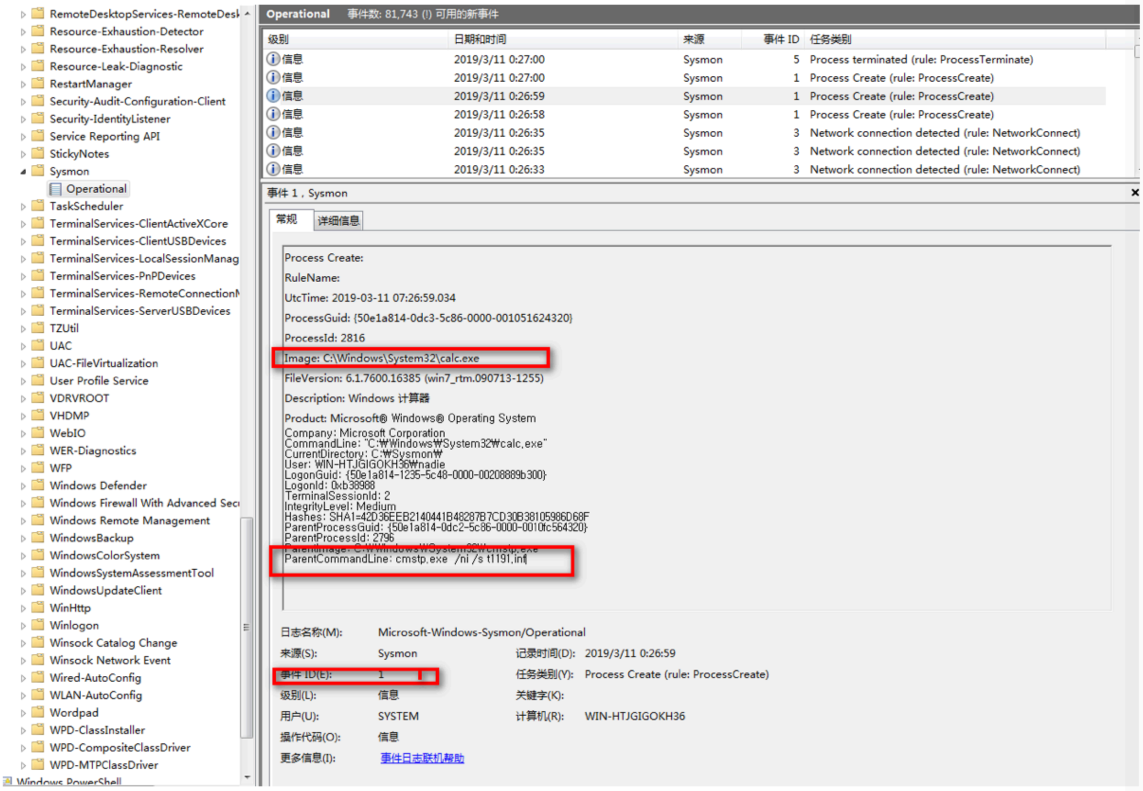
https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1191/T1191_uacbypass.inf

如下的组织曾经在攻击活动中使用过 cmstp:
Cobalt Group cmstp.exe /s /ns C:\Users\ADMINI~W\AppData\Local\Temp\XKNqbpzl.txt
MuddyWater cmstp.exe /s c:\programdata\DefenderService.inf

如果用 sysmon 日志来检测 cmstp.exe 相关的恶意行为，有三种规则可以使用：
CMSTP Execution 检测
１. Event 1 (Process creation)，进程创建事件，且 ParentImage 包含 CMSTP.exe or Event 3 (Network connection)网络连接事件 Image 包含 CMSTP.exe 且 DestinationIP is 属于外网地址.



```
Process Create:
RuleName:
UtcTime: 2019-03-11 07:26:59.034
ProcessGuid: {50e1a814-0dc3-5c86-0000-001051624320}
ProcessId: 2816
Image: C:\Windows\System32\calc.exe
FileVersion: 6.1.7600.16385 (win7_rtm.090713-1255)
Description: Windows 计算器
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
CommandLine: "C:₩Windows₩System32₩calc.exe"
CurrentDirectory: C:₩Sysmon₩
User: WIN-HTJGIGOKH36₩nadie
LogonGuid: {50e1a814-1235-5c48-0000-00208889b300}
LogonId: 0xb38988
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: SHA1=42D36EEB2140441B48287B7CD30B38105986D68F
ParentProcessGuid: {50e1a814-0dc2-5c86-0000-0010fc564320}
ParentProcessId: 2796
ParentImage: C:₩Windows₩System32₩cmstp.exe
ParentCommandLine: cmstp.exe  /ni /s t1191.inf
```



Operational 事件数: 81,743 (!) 可用的新事件

级别	日期和时间	来源	事件 ID	任务类别
信息	2019/3/11 0:27:00	Sysmon	5	Process terminated (rule: ProcessTerminate)
信息	2019/3/11 0:27:00	Sysmon	1	Process Create (rule: ProcessCreate)
信息	2019/3/11 0:26:59	Sysmon	1	Process Create (rule: ProcessCreate)
信息	2019/3/11 0:26:58	Sysmon	1	Process Create (rule: ProcessCreate)
信息	2019/3/11 0:26:35	Sysmon	3	Network connection detected (rule: NetworkConnect)
信息	2019/3/11 0:26:35	Sysmon	3	Network connection detected (rule: NetworkConnect)
信息	2019/3/11 0:26:33	Sysmon	3	Network connection detected (rule: NetworkConnect)

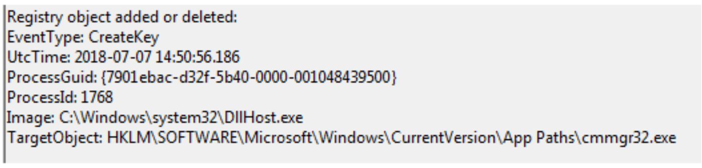
事件 1，Sysmon

```
Process Create:
RuleName:
UtcTime: 2019-03-11 07:26:59.034
ProcessGuid: {50e1a814-0dc3-5c86-0000-001051624320}
ProcessId: 2816
Image: C:\Windows\System32\calc.exe
FileVersion: 6.1.7600.16385 (win7_rtm.090713-1255)
Description: Windows 计算器
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
CommandLine: "C:₩Windows₩System32₩calc.exe"
CurrentDirectory: C:₩Sysmon₩
User: WIN-HTJGIGOKH36₩nadie
LogonGuid: {50e1a814-1235-5c48-0000-00208889b300}
LogonId: 0xb38988
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: SHA1=42D36EEB2140441B48287B7CD30B38105986D68F
ParentProcessGuid: {50e1a814-0dc2-5c86-0000-0010fc564320}
ParentProcessId: 2796
ParentImage: C:₩Windows₩System32₩cmstp.exe
ParentCommandLine: cmstp.exe  /ni /s t1191.inf
```

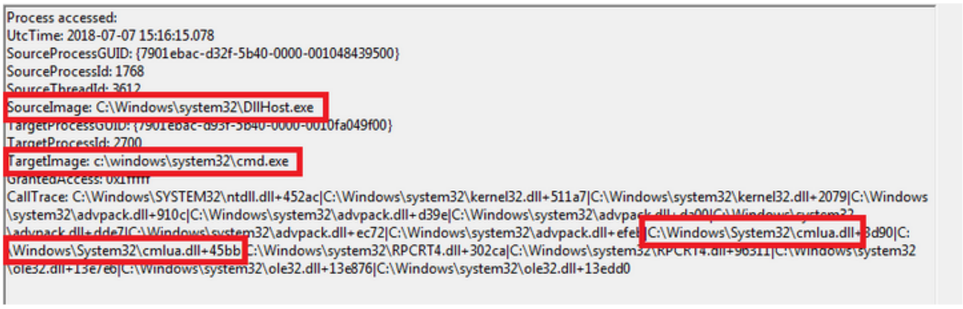
日志名称(M):	Microsoft-Windows-Sysmon/Operational		
来源(S):	Sysmon	记录时间(D):	2019/3/11 0:26:59
事件 ID(E):	1	任务类别(Y):	Process Create (rule: ProcessCreate)
级别(L):	信息	关键字(K):	
用户(U):	SYSTEM	计算机(R):	WIN-HTJGIGOKH36
操作代码(O):	信息		
更多信息(I):	事件日志联机帮助		

CMSTP UAC Bypass via COM Object Access 检测 uac bypass：

1 . Event 10 (ProcessAccess) 且 CallTrace 包含 CMLUA.dll or Event 12 or 13 (RegistryEvent) TargetObject 包含 CMMGR32.exe.

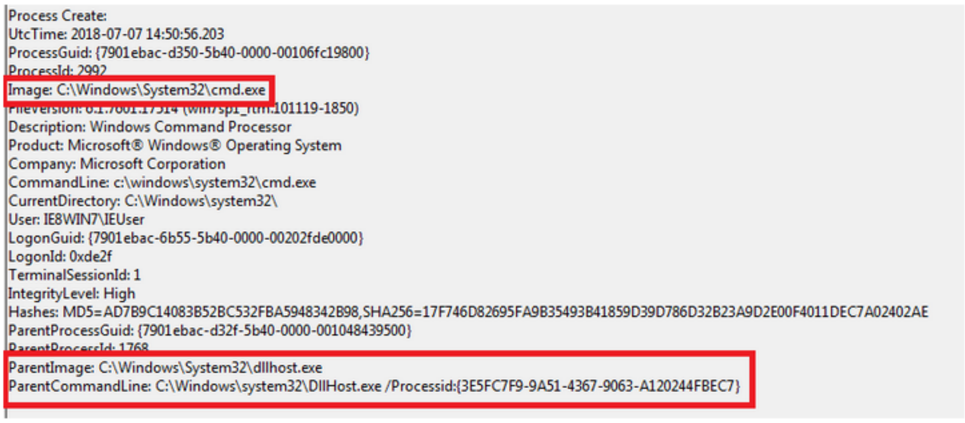


```
Registry object added or deleted:
EventType: CreateKey
UtcTime: 2018-07-07 14:50:56.186
ProcessGuid: {7901ebac-d32f-5b40-0000-001048439500}
ProcessId: 1768
Image: C:\Windows\system32\DllHost.exe
TargetObject: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\cmmgr32.exe
```



```
Process accessed:
UtcTime: 2018-07-07 15:16:15.078
SourceProcessGUID: {7901ebac-d32f-5b40-0000-001048439500}
SourceProcessId: 1768
SourceThreadId: 3612
SourceImage: C:\Windows\system32\DllHost.exe
TargetProcessGUID: {7901ebac-d93f-5b40-0000-0010fa049f00}
TargetProcessId: 2700
TargetImage: c:\windows\system32\cmd.exe
GrantedAccess: 0x1fffff
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+452ac|C:\Windows\system32\kernel32.dll+511a7|C:\Windows\system32\kernel32.dll+2079|C:\Windows
\system32\advpack.dll+910c|C:\Windows\system32\advpack.dll+d39e|C:\Windows\system32\advpack.dll+da00|C:\Windows\system32
\advpack.dll+dde7|C:\Windows\system32\advpack.dll+ec72|C:\Windows\system32\advpack.dll+efeb|C:\Windows\System32\cmlua.dll+3d90|C:
\Windows\System32\cmlua.dll+45bb|C:\Windows\system32\RPCRT4.dll+302ca|C:\Windows\system32\RPCRT4.dll+96311|C:\Windows\system32
\ole32.dll+13e7eb|C:\Windows\system32\ole32.dll+13e876|C:\Windows\system32\ole32.dll+13edd0
```

2 . Event 1 ， ParentCommandLine 包含 dllhost.exe 且 包含 CMSTPLUA COM object GUID (3E5FC7F9-9A51-4367-9063-A120244FBEC7) 或者 CMLUAUTIL (3E000D72-A845-4CD9-BD83-80C07C3B881F).



```
Process Create:
UtcTime: 2018-07-07 14:50:56.203
ProcessGuid: {7901ebac-d350-5b40-0000-00106fc19800}
ProcessId: 2992
Image: C:\Windows\System32\cmd.exe
FileVersion: 6.1.7601.17514 (win7sp1_rtm.101119-1850)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
CommandLine: c:\windows\system32\cmd.exe
CurrentDirectory: C:\Windows\system32\
User: IE8WIN7\IEUser
LogonGuid: {7901ebac-6b55-5b40-0000-00202fde0000}
LogonId: 0xde2f
TerminalSessionId: 1
IntegrityLevel: High
Hashes: MD5=AD7B9C14083B52BC532FBA5948342B98,SHA256=17F746D82695FA9B35493B41859D39D786D32B23A9D2E00F4011DEC7A02402AE
ParentProcessGuid: {7901ebac-d32f-5b40-0000-001048439500}
ParentProcessId: 1768
ParentImage: C:\Windows\System32\dllhost.exe
ParentCommandLine: C:\Windows\system32\DllHost.exe /Processid:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}
```