Open in app ↗ Sign up Sign in

Medium Search Write

Lateral Movement: Abuse the Power of DCOM Excel Application

Raj Patel · Follow

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 $/month

TCP/IP for its network communications; specifically, it uses the `ncacn_ip_tcp` protocol sequence, where:

- `ncacn` stands for "Connection-Oriented Network Computing Architecture."
- `ip_tcp` specifies the use of TCP/IP.

In practical terms, when you see this protocol sequence, it indicates that RPC is using TCP/IP for network communications in a connection-oriented

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month

The basic flow of communication is like this:

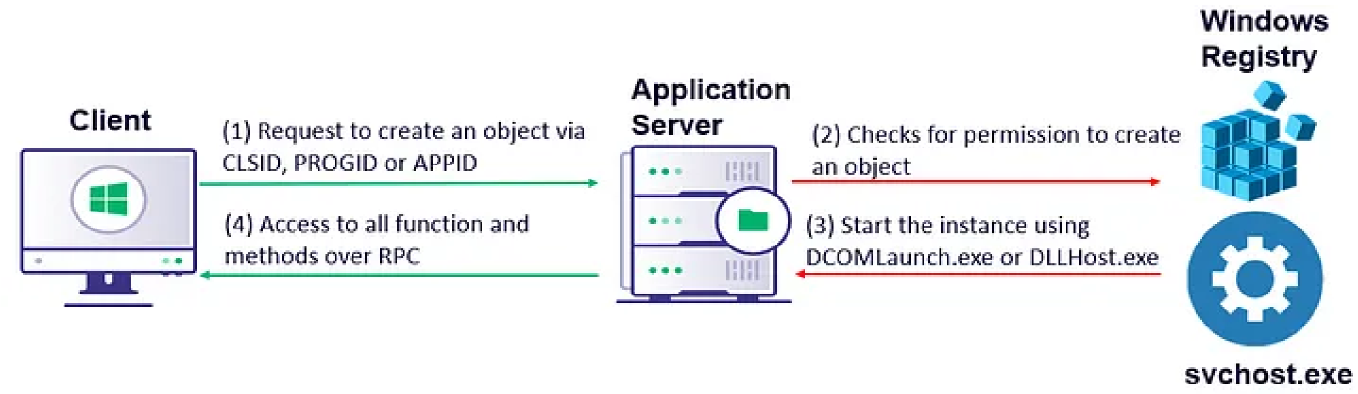

Client
(1) Request to create an object via CLSID, PROGID or APPID
(4) Access to all function and methods over RPC
Application Server
(2) Checks for permission to create an object
(3) Start the instance using DCOMLaunch.exe or DLLHost.exe
Windows Registry
svchost.exe

Figure 01 — DCOM flow over the network

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Sign up for free

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

Try for 5 $/month

- Ability to remotely write a file in the system *PATH*
- Tested on Windows 10 and 11
- Tested on 64-bit installation of Office 365

While enumerating different methods of Excel objects, we discovered the ***ActivateMicrosoftApp()*** method could be used to get shell access because Microsoft still supports activation of some end of life (EOL) software such as FoxPro, Schedule Plus, and Office Project. It is unlikely that any of these

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

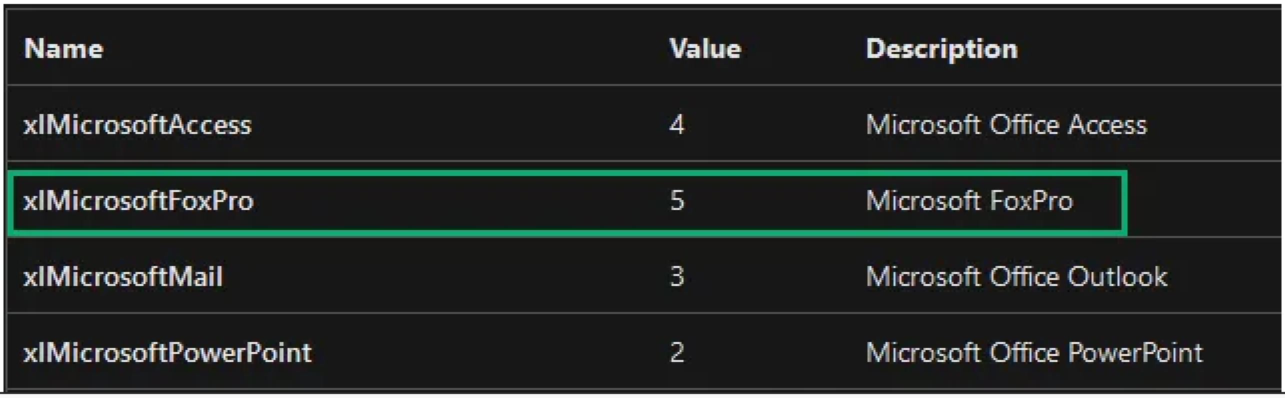
✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month

ActivateMicrosoftApp() method takes one parameter which specifies the Microsoft application to activate.



Name	Value	Description
xlMicrosoftAccess	4	Microsoft Office Access
xlMicrosoftFoxPro	5	Microsoft FoxPro
xlMicrosoftMail	3	Microsoft Office Outlook
xlMicrosoftPowerPoint	2	Microsoft Office PowerPoint

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month

However, if the application is not present on the system ***ActivateMicrosoftApp()*** will throw an error that it “Cannot run ‘*FOXPROW.exe*’. The program or one of its components is damaged or missing.” After some research, we utilized Process Monitor to further investigate underlying operations.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 $/month

folder, then our malicious binary will execute and provide us access to the target machine.

```
copy c:\windows\system32\calc.exe '\\192.168.49.160\c$\users\user\AppData\local\Micr

$com = [System.Activator]::CreateInstance([type]::GetTypeFromProgID("Excel.Applicati

$com.ActivateMicrosoftApp("5")
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 $/month

Figure 06 — Error thrown if ProgID could not map to CLSID

Alternatively, we could use CLSID instead of ProgID to identify the Excel COM class object. Please note that CLSID can differ between various

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Sign up for free

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

Try for 5 $/month

PowerShell script that initializes an instance of the Excel.Application object via DCOM and invokes the ***ActivateMicrosoftApp()*** method on the localhost. Then, create a scheduled task configured to run at specific intervals, which will execute the PowerShell script we created. Ultimately, ensure that *FOXPROW.exe* is placed within the system *PATH* and wait for the scheduled task to execute.

```
PS C:\Users\User\Desktop> cat .\ExcelPersistence.ps1
$com = [System.Activator]::CreateInstance([type]::GetTypeFromProgID("Excel.Applicati
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 $/month

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 $/month

Note: The initial location where the *ActivateMicrosoftApp()* method searches for *FOXPROW.exe* is within the C:\Program Files\Microsoft Office\root\Office16 folder.

Impact

This technique can have a significant impact since it allows attackers to execute malicious executable on any machine that has Microsoft Office installed, given administrative rights to that machine. It could be abused by attackers in a ransomware scenario. The malicious actor has the capability to upload malware, place it within the *PATH*, and then run the malware by

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month

To detect this attack, defenders can look for a child process spawning off of *Excel.exe*. If the following processes are spawned as a child process of *Excel.exe*, then you should investigate further:

- FOXPROW.exe
- SCHDPLUS.exe
- WINPROJ.exe

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month

your environment, you might want to investigate it further.

To learn more about security of DCOM read here.

Mitigation

To mitigate this attack, consider configuring the user identity located under Component Services > Computers > My Computer > DCOM Config > Microsoft Excel Application > Properties. There are three options available:

- The interactive user — runs Excel as the currently logged on user's

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 $/month

Big thanks to Duane Michael, Jared Atkinson, Matt Nelson and others who have helped review the blog post. Please reach out on X for your thoughts. I am curious to know other creative ways this technique could be abused. Thank you for reading!

Lateral Movement Specterops Dcom Excel Research

--

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month