.. /Rasautou.exe

Execute (DLL)

Windows Remote Access Dialer

Paths:
C:\Windows\System32\rasautou.exe

Resources:
- https://github.com/fireeye/DueDLLigence
- https://www.fireeye.com/blog/threat-research/2019/10/staying-hidden-on-the-endpoint-evading-detection-with-shellcode.html

Acknowledgements:
- FireEye (@FireEye)

Detections:
- Sigma: https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/process_creation/win_rasautou_dll_execution.yml
- IOC: rasautou.exe command line containing -d and -p

Execute

Loads the target .DLL specified in -d and executes the export specified in -p. Options removed in Windows 10.

```
rasautou -d powershell.dll -p powershell -a a -e e
```

Use case:	Execute DLL code
Privileges required:	User, Administrator in Windows 8
Operating systems:	Windows vista, Windows 7, Windows 8, Windows 8.1
ATT&CK® technique:	T1218
Tags:	Execute: DLL