.. /Forfiles.exe

Execute | Alternate data streams

Selects and executes a command on a file or set of files. This command is useful for batch processing.

Paths:
C:\Windows\System32\forfiles.exe
C:\Windows\SysWOW64\forfiles.exe

Resources:
- https://twitter.com/vector_sec/status/896049052642533376
- https://gist.github.com/api0cradle/cdd2d0d0ec9abb686f0e89306e277b8f
- https://oddvar.moe/2018/01/14/putting-data-in-alternate-data-streams-and-how-to-execute-it/

Acknowledgements:
- Eric (@vector_sec)
- Oddvar Moe (@oddvarmoe)

Detections:
- Sigma: proc_creation_win_lolbin_forfiles.yml

Execute

Executes calc.exe since there is a match for notepad.exe in the c:\windows\System32 folder.

```
forfiles /p c:\windows\system32 /m notepad.exe /c calc.exe
```

Use case: Use forfiles to start a new process 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: T1202: Indirect Command Execution

Alternate data streams

Executes the evil.exe Alternate Data Stream (AD) since there is a match for notepad.exe in the c:\windows\system32 folder.

```
forfiles /p c:\windows\system32 /m notepad.exe /c "c:\folder\normal.dll:evil.exe"
```

Use case: Use forfiles to start a new process from a binary hidden in an alternate data stream
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1564.004: NTFS File Attributes